数学基礎論講義

Lectures on Foundations of Mathematics

不完全性定理とその発展

日本評論社

はじめに

本書は不完全性定理を主題とする数学基礎論の入門書である．

「数学基礎論」は，ゲーデルの二つの定理 —— 完全性定理 (1930 年) と不完全性定理 (1931 年) —— を主な出発点として 1960 年代から 70 年代に大きな発展を遂げた，現代数学のなかでも比較的新しい分野である．70 年代以降は計算機科学との交流の活発化やその他数理科学への広範な応用により，単に「ロジック」と呼ばれることが多くなっているが，本書は原点に立ち返るというつもりであえて「数学基礎論講義」と称することにした．

本書を構成する 4 つの講義シリーズ (パート A, B, C, D) および補講は 4 人の基礎論研究者によって別々に書かれたもので，それぞれ異なるアングルから不完全性定理を中心とする数学基礎論の一姿を捉えている．各パートは独立に読むこともできるが，これらを合わせてできる立体像こそがこの本で真に伝えたいものである．主な読者対象としては，学部上級から大学院初年級程度の学生 (とくに数学や情報科学を専攻するもの) を考えているが，不完全性定理や数学基礎論に興味がある方なら誰でも自分なりの読みかたで役立てていただけると思う．

まず，4 つのパートの内容をそれぞれ簡単に紹介しておこう．

数理論理学の基礎知識を私，田中がパート A にまとめた．しかし，ここからていねいに読み始める必要はない．基礎論に興味を持つ人は妙に細かなことにこだわる癖があるようだが，何でも大局的な視点をもつことが第一に大切であり，そのためにはある程度ずぼらな方がいいこともある．ただし，専門家を目指すなら，この程度の知識は宴会で酔っぱらってもそらんじられるくらいにマスターしておきたい．そうでないと，基礎論の研究者とは付き合えないだろう．なお，最後の 2 節 (4.5 と 4.6) は，当初パート B の一部として書かれていたものなので，原作者は鹿島氏である．

パート B では，不完全性定理をオーソドックスな流れに沿って解説する．執筆は

鹿島亮氏である．不完全性定理には第一定理と第二定理があり，後者に対してゲーデルは証明のアイデアを述べただけで，証明の詳細を生涯発表しなかった．ゲーデルのあとヒルベルト・ベルナイスの研究を経て，レーブらの仕事によって第二不完全性定理の見通しの良い証明が完成したのは 1950 年代も半ばである．その証明の鍵になるのは，可導性条件 (Derivability Conditions) と呼ばれるもので，これについての研究はソロベイ，ブーロスらの今日の仕事につながっている．このパートでは，不完全性定理の証明をわかりやすくかつ正確に述べると共に，それに関わる最近の研究を展望する．

不完全性定理の発見以来約半世紀を経た 1977 年，ペアノ算術における新しい独立命題 (証明も反証もできない命題) をパリスとハーリントンが発見した．パート C では，彼らの結果をはじめ，ペアノ算術やその部分体系から独立な種々の組合せ命題について詳説する．執筆担当は角田法也氏である．パリスとハーリントンはモデル論を使ってその独立性を証明したが，この本の証明はケトーネンとソロベイが開発した証明論プラス計算論の手法による．また，このパートで扱うグッドシュタイン列の停止性，ヒドラ-ヘラクレス戦の決定性などの独立命題は，ある種の自然なアルゴリズムの停止性に関するものであり，計算の理論においても重要な意味を持っている．

パート D では，算術のモデルに関連する多くの研究の中から不完全性定理の本質を捉えた成果を選りすぐって紹介する．執筆は菊池誠氏である．不完全性定理といえば，まずシンタックス (証明論) の話と思われるだろうが，最近はセマンティクス (モデル論) の視点から議論することも多くなっている．モデルを使った第 2 不完全性定理の証明については，菊池氏自身が学位論文のなかで考案したものもあるが，ここでは集合論研究者イェックの新しい証明を多少アレンジして紹介している．さらに，計算量理論との関係で注目されているウィルキーらの研究の一端にも触れる．

最後に，私が担当した補講では，ヒルベルトのプログラムの現代版といわれる「逆数学プログラム」を簡単に紹介し，また不完全性定理に関する 2, 3 の注意を述べる．補講の目的は，不完全性定理のまわりにまだたくさんのおもしろい課題が

残されていることを知っていただくことで,「逆数学」はその一例にすぎない．これらの話題については，別の機会にまた詳しく述べたいと思っている．

本書の共同執筆の構想がおよそ固まったのは，1994 年の秋くらいのことである．それ以前から，編者は一人でこのような本を書き下ろすつもりだったのだが，参考になる資料が少なく，言葉遣いから証明法に至るまですべてを考え直さねばならず手に余っていた．そうこうするうちに，私の学生たち (鹿島氏，菊池氏) がこの分野のエクスパートに成長し，また友人の角田氏も協力してくれることになった．じつは，この本をもっとも必要としていたのは学生時代の彼らであり，私は最初彼らに請われて本を書く気になったのである．それをこうして彼ら自身が書くというのは，まことに「不完全性定理」の本に相応しい話である．ともあれ，出版まで漕ぎ着けたのは彼ら 3 人の熱意と誠意のお陰である．しかし，本書を通じて見落としや間違いがあればもちろん編者の責任である．

言葉遣いについて付け加えると，本書では，recursive に「再帰的」，provability に「可証性」などという訳語を当てている．従来 recursive には「帰納的」という訳語を使うことが多かったが，専門用語の上ではどうしても inductive との区別が必要になるので，この本ではやや強引に recursive =「再帰的」で統一した．

本書の編集作業の大半は，私がオックスフォード大の数学研究所に滞在した 95 年の約半年間になされた．オックスフォード大のウィルキー博士らには，快適な研究環境を提供していただき，ここに感謝の意を表したい．また国内外の諸先輩方や多くの友人たち，そして学生諸君からも様々な形でご協力いただいた．一人一人の名前をあげることはできないが皆さんに心から感謝している．最後に，日本評論社の亀井哲治郎さん，大賀雅美さんには，編集校正ばかりでなく本が完成するまでのさまざまな段階でわれわれ 4 人の相談相手になっていただいたこと，大変ありがたく思っている．

平成 8 年 12 月　仙台にて

田中一之

目次

Part A. 数理論理学入門

このパートの目的は，本書全体を読むのに必要かつ十分な数理論理学の知識を整理して提供することである．中心となる題材は，1 階述語論理の完全性 (ゲーデル (K. Gödel) の完全性定理) と，再帰的 (recursive) 関数および再帰的集合の基本的な性質である．ロジックの入門講義をどこか受けられた方には常識になっているはずのものだが，完全性定理くらいまで一通り勉強したという人でも肝心なところでの見落しや誤解をしていることがよくあるので，とりあえず次のテストで理解の確認をしていただきたい．初心者の方は，問題文だけでも頭に入れておくと，先の理解の助けになるだろう．

問 1． ある形式体系 T において，論理式 $\exists x\varphi(x)$ が証明できても，$\varphi(t)$ が証明できるような項 t が存在するとは限らない．そのような体系 T と論理式 $\exists x\varphi(x)$ の例をあげよ．

上の問題ができないと，“ヘンキン (L.Henkin) の定数記号” を用いた完全性定理の証明は何をやっているのかわからないと思う．

問 2． 共通部分を持たない 2 つの RE (再帰的枚挙可能) 集合 A, B で，次の性質を持つものが存在することを示せ．どんな再帰的 (recursive) 集合 C も，A の真部分集合になるか，B の真部分集合になるか，あるいは A と B との両方に交わる．すなわち，A を含み，B との共通部分が空になるような再帰的集合 C は存在しない．(このとき，A と B とは**再帰的に分離不能**であるという．)

再帰理論におけるもっとも基本的な事実は，再帰的でない RE 集合が存在することであり，それは第一不完全性定理のエッセンスでもある．その証明法をご存知なら，上の問題はその簡単な応用問題になっているので解いてみてほしい．ま

た，この問題の主張は第一不完全性定理の強いバージョン (本質的な決定不能性) に対応しており，パート D でも用いられる．

第 1 講　準備練習

1.1　論理について

この本全体を通じて，われわれの議論の土台となるのは，あらゆる命題は真か偽かのいずれか一方に定まるという 2 値論理である．数学の世界の 99 パーセントはこの論理の上に築かれており，われわれの立場も他の数学分野に較べて，特に厳密とか，用いる論理に制約があるというわけではない．

数学の議論を展開するためには，論理記号として次の 6 つがあれば十分である．

否定記号	$\neg$	($\cdots$ でない)
連言記号	$\wedge$	(かつ)
選言記号	$\vee$	(または)
含意記号	$\rightarrow$	(ならば)
全称記号	$\forall$	(任意の $\cdots$ について)
存在記号	$\exists$	(ある $\cdots$ について)

大学で数学や計算機科学の講義を受けたことがある人なら，とくに論理の勉強をしていなくても，これらの論理記号の使い方や基本的な性質についてある程度ご存知かと思う．そこで，論理のいろはの説明はやめて，最初から練習問題を考えていこう．ここでは解析学の初学者を悩ませる ε-δ 論法を題材にするが，ε-δ 論法自体を知らなくても差し支えはない．(注意： 論理 (記号) が使えることと，論理の仕組みがわかることは別である．それは，整数の足し算や掛け算が正確にできても，整数全体が「環」と呼ばれる代数構造であると理解したわけではないのと同じである．論理の仕組みについては，次講以降で述べる．)

「実数から実数への関数 $f(x)$ が $x = x_0$ で連続である」ということを，いわゆる ε-δ 論法では

(1) 「任意の $\varepsilon > 0$ に対して，ある $\delta > 0$ が存在して，$|x - x_0| < \delta$ となるすべての x について，$|f(x) - f(x_0)| < \varepsilon$ となる」

と表現する．この文を上の論理記号を使って，書き直してみよう．少しひっかか

るのは,「$|x-x_0|<\delta$ となるすべての x について」のところだが，それは「各 x について，それが $|x-x_0|<\delta$ を満たすならば」と解釈し直せばよい．すると，(1) は以下のように記号だけで表現できる:

(2) $\forall\varepsilon>0\,\exists\delta>0\,\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$.

さらに，全称記号，存在記号を標準的な形に直して，

(2′) $\forall\varepsilon(\varepsilon>0\rightarrow\exists\delta(\delta>0\wedge\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)))$.

と書くこともできる．

連続性がなぜ (1) のように表せるかは解析学の本を見ていただくことにし，ここでは (1) ⇔ (2) ⇔ (2′) の書き換えについて完全にマスターしてほしい．これは慣れだけの問題だから，自分が納得のいくまで紙に書くなどして，手で覚えればよい．この例に限らず，ε-δ 論法における定義や定理はすべて 6 つの論理記号だけを使った論理式で表現できてしまう．じつは，このような論理 (記号) の枠組みで解析学を展開する方法が ε-δ 論法に他ならない．さらにいえば，現代数学のあらゆる分野 (数学基礎論も) がこれらの論理の上に組み立てられている．大学以上の数学の教科書なら何でもよいから，そこから定義や定理をいくつか取り出して，論理式に翻訳してみるといいだろう．

問題．「関数 $f(x)$ がすべての点で連続である」と「関数 $f(x)$ がすべての点で一様連続である」をそれぞれ論理式で表し，両者を比較せよ．

次は，論理の基本法則を使った書き換えの練習である.「関数 $f(x)$ が $x=x_0$ で連続でない」ということを論理式で表現することを考える．まず，単純な答えとして，

(3) $\neg\forall\varepsilon>0\,\exists\delta>0\,\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$

も間違いではないが，もう少し役立つ形に直してほしい．(1) の否定文を日本語で作ってから記号化する方法もあるが，それは以下で示す記号操作よりよほどむずかしいし，また間違いも起こりやすい．論理式 (3) は以下のように変形していく

ことができる．

$$\neg\forall\varepsilon>0\,\exists\delta>0\,\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$$
$$\Leftrightarrow\exists\varepsilon>0\,\neg\exists\delta>0\,\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$$
$$\Leftrightarrow\exists\varepsilon>0\,\forall\delta>0\,\neg\forall x(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$$
$$\Leftrightarrow\exists\varepsilon>0\,\forall\delta>0\,\exists x\,\neg(|x-x_0|<\delta\rightarrow|f(x)-f(x_0)|<\varepsilon)$$
$$\Leftrightarrow\exists\varepsilon>0\,\forall\delta>0\,\exists x(|x-x_0|<\delta\wedge\neg|f(x)-f(x_0)|<\varepsilon)$$
$$\Leftrightarrow\exists\varepsilon>0\,\forall\delta>0\,\exists x(|x-x_0|<\delta\wedge|f(x)-f(x_0)|\geqq\varepsilon)$$

この変形について簡単に説明しておこう．

- $\neg\forall\varepsilon>0\cdots$ は，$\exists\varepsilon>0\,\neg\cdots$ と同値である．なぜなら,「(すべての $\varepsilon>0$ に対して $\cdots$) ではない」ことは,「$\cdots$ でない $\varepsilon>0$ が存在する」ことだから．
- $\neg\exists\delta>0\cdots$ は，$\forall\delta>0\,\neg\cdots$ と同値である．なぜなら,「$\cdots$ となる $\delta>0$ が存在しない」ことは,「どんな $\delta>0$ に対しても $\cdots$ でない」ことだから．
- $\neg\forall x\cdots$ は，$\exists x\,\neg\cdots$ と同値である．
- $\neg(\phi\rightarrow\psi)$ は，$\phi\wedge\neg\psi$ と同値である．なぜなら,「(ϕ であれば ψ である) が成り立たない」ことは,「ϕ であっても ψ でない」ことだから．
- $x<y$ の否定は $x\geqq y$ である．

変形で得られた最後の行を日本語に戻せば，

(4)「ある $\varepsilon>0$ が存在して，どんな $\delta>0$ に対しても，$|x-x_0|<\delta$ かつ $|f(x)-f(x_0)|\geqq\varepsilon$ となる x が存在する」

となる．(1) の否定文として (4) が得られたわけだが，記号翻訳を介さないで (1) から直接 (4) を導くのは相当むずかしいと思う．ある関数が連続でないことを証明するには (4) の形が実際に必要になるから，解析学を学ぶにはまず論理計算に慣れておくことが大切なのである．

ここで，上の式変形に使った法則を含めて，否定に関する基本法則をまとめておこう．

(a) $\neg\neg\phi\Leftrightarrow\phi$

(b) $\neg(\phi\wedge\psi)\Leftrightarrow\neg\phi\vee\neg\psi$

(c) $\neg(\phi \lor \psi) \Leftrightarrow \neg\phi \land \neg\psi$

(d) $\neg(\phi \to \psi) \Leftrightarrow \phi \land \neg\psi$

(e) $\neg\forall x\, \phi \Leftrightarrow \exists x\, \neg\phi$

(f) $\neg\exists x\, \phi \Leftrightarrow \forall x\, \neg\phi$

特に，(b), (c), (e), (f) はド・モルガン (**De Morgan**) の法則と呼ばれる．

上の法則のもう一つの重要な応用は，ある論理記号を別の記号によって置き換える，または定義することである．たとえば，与えられた論理式において，そのなかに現れる $\phi \land \psi$ を $\neg(\phi \to \neg\psi)$ に，$\phi \lor \psi$ を $\neg\phi \to \psi$ に，$\exists x\, \phi$ を $\neg\forall x\, \neg\phi$ に置き換えれば，論理記号として $\neg$, $\to$, $\forall$ だけを含む式ができる．したがって，$\neg$, $\to$, $\forall$ の 3 つの論理記号に関する法則が完全にわかれば，$\land$, $\lor$, $\exists$ に関することはそれから付随的に導ける．たとえば，$(\phi \land \psi) \to (\phi \lor \psi)$ が成り立つかどうかは，$(\neg(\phi \to \neg\psi)) \to (\neg\phi \to \psi)$ が成り立つかどうかを見ればよい．どの論理記号を基本に選ぶべきは一概にいえないが，このパートではおもに $\neg$, $\to$; $\forall$ に基づく論理体系について述べる．また，上の 6 つ以外の論理記号も必要に応じて導入する．たとえば，$\phi \leftrightarrow \psi$ は $(\phi \to \psi) \land (\psi \to \phi)$ の略記と定義する．

最後に，論理式の解釈について，一言述べておく.「すべての x に対して」というような量化を行う場合，議論の対象は暗黙に限定されている．上の例の (1) や (2) では，対象は実数の範囲であることが仮定されている．同じ論理式でも，扱う対象の範囲により真偽値が異なったり，解釈ができなくなることがある．このあたりの厳密な議論は第 3 講の述語論理のところで行なう．

1.2 集合について

集合の表し方には，その要素を列挙する外延的定義方式 $\{a, b, \cdots, c\}$ と，条件を記述する内包的定義方式 $\{x : P(x)\}$ がある．たとえば，$\{2, 4, 6, 8\}$ と $\{x : x$ は偶数かつ $0 < x < 10\}$ は同じ集合の別表現である．また，$\{\quad\}$ と $\{x : x \neq x\}$ はどちらも要素を持たない集合で，それを空集合と呼び，$\emptyset$ で表す．

集合 A が要素 x をもつとき，$x \in A$ と記す．集合 A のすべての要素 x が集合 B にも属するとき，すなわち，$\forall x(x \in A \to x \in B)$ のとき，A は B の**部分集合**

であるといい，$A \subset B$ または $A \subseteqq B$ と書く．そして，$A \subset B$ かつ $B \subset A$ のとき，$A = B$ と定義する．$A \subset B$ だが，$A \neq B$ のとき，A は B の**真部分集合**であるという．

集合 $A = \{x : P(x)\}$, $B = \{x : Q(x)\}$ が与えられたとき，それらから第 3 の集合を作る操作として，交わり $\cap$, 結び $\cup$, 差 $-$ を以下のように定義する:

$$A \cap B = \{x : P(x) \wedge Q(x)\},$$

$$A \cup B = \{x : P(x) \vee Q(x)\},$$

$$A - B = \{x : P(x) \wedge \neg Q(x)\}.$$

ある特定の議論の対象となるもの全体の集合 (宇宙と呼ぶ) を U とするとき，集合 $A \subset U$ に対して，$U - A$ を単に $\bar{A}$ と書いて，A の**補集合**という．宇宙 U の定め方は便宜的であって，いつでも適当な宇宙がとれるという保証はない．実際，集合全体の宇宙などは (集合として) 存在し得ないことが知られている．論理のド・モルガンの法則から，集合に関する次のド・モルガンの法則が導ける:

$$\overline{(A \cap B)} = \bar{A} \cup \bar{B},$$

$$\overline{(A \cup B)} = \bar{A} \cap \bar{B}.$$

問題．上の等式を証明せよ．

集合 A が与えられたとき，その部分集合全体からなる集合 $\{X : X \subset A\}$ を A の**ベキ集合** (**power set**) と呼んで，$P(A)$ または 2^A で表す．たとえば，$A = \{a, b, c\}$ のとき，$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$ である．一般に，A が n 個の要素からなるとき，$P(A)$ は 2^n 個の要素をもつ．

n 個の集合 $A_1, A_2, \cdots, A_n$ から 1 つずつ要素 $a_i \in A_i$ を取り出して並べたもの $(a_1, a_2, \cdots, a_n)$ を ***n*-組** (***n*-tuple**) といい，n-組全部の集まりを $A_1 \times A_2 \times \cdots \times A_n$ で表す．このとき，どれかの A_i が空集合なら，$A_1 \times A_2 \times \cdots \times A_n$ も空である．$A_1 = A_2 = \cdots = A_n = A$ のとき，$A_1 \times A_2 \times \cdots \times A_n$ を A^n と書く．特に，A^1 は A と同一視する．A^0 は空な組 ( ) だけを要素とする集合 $\{(\ )\}$ である．これを空集合 $\{\}$ と混同してはならない．

A^n の部分集合 R は A 上の n 項関係 (**relation**) または述語 (**predicate**) と呼ばれる．関係と述語の用法を区別し，関係 $R = \{(x_1, \cdots, x_n) : Q(x_1, \cdots, x_n)\}$ を定める論理式 Q を述語という場合もあるが，われわれは両者を区別しないで用いる．そして，$(x_1, \cdots, x_n) \in R$ を $R(x_1, \cdots, x_n)$ と表したり，特に R が 2 項関係のときは $x_1 R x_2$ と書くこともある．等号 $=$ は $\{(x, y) : x = y\}$ と同じとみなせる．

集合 X の各要素に集合 Y のある要素を対応させる**関数**を $f : X \to Y$ で表す．このとき，X を f の**定義域** $\mathrm{dom}(f)$, $f(X) = \{f(x) : x \in X\}$ を f の**値域** $\mathrm{range}(f)$ という．関数 $f : X \to Y$ に対して，$X \times Y$ の部分集合 $\{(x, f(x)) : x \in X\}$ を f のグラフ (**graph**) という．逆に，$X \times Y$ の部分集合 F が，各 $x \in X$ に対し $(x, y) \in F$ となる y をちょうど 1 つ定めるなら，F をグラフとする関数がただ一つ存在する．

対象全部の集合 U を固定し，その部分集合 A が与えらたとする．このとき，

$$\chi_A(x) = \begin{cases} 1, & x \in A \text{ のとき} \\ 0, & x \notin A \text{ のとき} \end{cases}$$

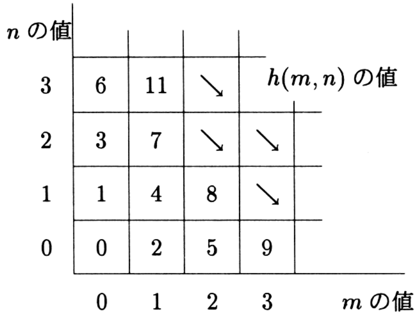
で定義される関数 $\chi_A : U \to \{0, 1\}$ を集合 A の**特性関数** (**characteristic function**) という．逆に，$f : U \to \{0, 1\}$ が与えられたとき，f を特性関数とするような集合がただ一つ定まる．集合 A とその特性関数 χ_A はしばしば同一視する．

2 つの集合 A, B の各要素の間に 1 対 1 対応があれば，A と B は同じ**濃度** (**cardinality**) をもつという．ある自然数 n について，集合 A と集合 $\{0, 1, \cdots, n-1\}$ が同じ濃度をもつとき，A は**有限集合**であるといい，その濃度は n であるという．有限でない集合を**無限集合**と呼ぶ．集合 A が自然数全体 $\mathbf{N}$ と同じ濃度をもつとき，A の濃度は $\aleph_0$ (アレフ·ゼロ) であるという．有限集合と濃度 $\aleph_0$ の集合を合わせて (**高々**) **可算集合**と呼び，それ以外を**非可算集合**と呼ぶ．選択公理と呼ばれるやや自明性に欠ける命題を仮定すると，どんな無限集合 A も自らと同じ濃度の真部分集合を含むこと (デデキントの意味での無限性) がいえる．

可算集合と非可算集合の代表的な例を二，三示しておこう．まず，自然数のペア (2-組) 全体 $\mathbf{N}^2$ の濃度は $\aleph_0$ である．なぜなら，次の関数 h は $\mathbf{N}^2$ から $\mathbf{N}$ の

上への 1 対 1 関数 (全単射) である:

$$h(m,n) = \frac{(m+n)(m+n+1)}{2} + m.$$



問題．$\mathbf{N}^3$ が濃度 $\aleph_0$ をもつことを示せ．

次に，有理数全体の集合 $\mathbf{Q}$ が濃度 $\aleph_0$ をもつことを示そう．有理数を既約分数 $\frac{m}{n}$ または $-\frac{m}{n}$ で表し，これらと $(0,m,n)$ または $(1,m,n)$ を対応づければ，$\mathbf{Q}$ は $\mathbf{N}^3$ の部分集合と同じ濃度になる．したがって，上の問題により，$\mathbf{Q}$ は $\mathbf{N}$ の部分集合とも同じ濃度になる．$\mathbf{N}$ の無限部分集合は，その各要素を大きさの順に並べることで，$\mathbf{N}$ 全体と 1 対 1 対応になるから，結局 $\mathbf{Q}$ と $\mathbf{N}$ も同じ濃度をもつ．

非可算集合の例として，$\mathbf{N}$ のベキ集合 $P(\mathbf{N})$ を考える．いま，$P(\mathbf{N})$ と $\mathbf{N}$ が 1 対 1 に対応していると仮定して矛盾を導こう．まず，$n \in \mathbf{N}$ に対応する $\mathbf{N}$ の部分集合を A_n と書く．そして，$B = \{n : n \notin A_n\}$ とおく．B は $\mathbf{N}$ の部分集合だから，ある $m \in \mathbf{N}$ が存在して，$A_m = B$ となるはずである．このとき，m は B の要素になるか否か？ $m \in B$ とすると，m は B の内包条件を満たすはずだから，$m \notin A_m$, つまり $m \notin B$ となって矛盾．逆に，$m \in B$ でないとすると，すなわち $m \notin A_m$ だから，m は B に属することになり，やはり矛盾．したがって，$P(\mathbf{N})$ と $\mathbf{N}$ が同じ濃度をもつという仮定が否定された．このような証明法を対角線論法 (**diagonal argument**) と呼ぶ．

問題. 対角線論法で，実数全体の集合 $\mathbf{R}$ が非可算になることを証明せよ．ヒント：実数の集合 $\mathbf{R}$ と $\mathbf{N}$ が 1 対 1 に対応していると仮定して，各 $n \in \mathbf{N}$ に対応する実数 α_n と小数第 n 位で異なる実数 β を定義せよ．

上の問題で示されるように，$\mathbf{N}$ と $\mathbf{R}$ は濃度が異なる．では，$\mathbf{N} \subset A \subset \mathbf{R}$ となる集合 A で，$\mathbf{N}$ とも $\mathbf{R}$ とも濃度が異なるものは存在するかというのが，1900 年にヒルベルト (D. Hilbert) が提起した 23 問題の筆頭である．存在しないという側の主張が**連続体仮説**と呼ばれているが，現在知られている集合論の公理系では，この命題の肯定も否定も証明できないことがわかっている (1938 年のゲーデル，1963 年のコーエン (P. Cohen) の仕事による)．

1.3 再帰的定義と帰納法による証明

漸化式 (隣接項間の関係) で与えられた数列の一般項を求める問題は，高校数学で馴染み深い．たとえば，

$$f(n+1) = f(n) + n + 1, \quad \text{ただし } f(0) = 1$$

の解は，

$$f(n) = \frac{1}{2} \cdot (n^2 + n + 2)$$

である．漸化式による定義では関数 f を定義するのに f 自身を用いているわけだから，その正当性には多少疑念を生じる余地がある．しかし，漸化式にしたがって，下から順に $f(0), f(1), f(2), \cdots$ と計算していくことで任意の n について $f(n)$ がただ一つ定まるから，これはこれで正しい定義には違いない．このような定義方法を一般化して，**(原始) 再帰的定義**という．再帰的および原始再帰的定義は第 4 講において形式化され，両者はそこで峻別されるが，ここではそれらを区別せず，素朴に (インフォーマルに) 議論を進める．

再帰的な定義がなされるのは，関数ばかりでない．たとえば，非負偶数の集合 E を次のように再帰的に定義することができる：

(1) $0 \in E$

(2) $n \in E$ ならば $n + 2 \in E$

(3) (1), (2) から有限ステップで得られるものだけが E に属する．

すなわち，E は 0 を含み (条件 1), +2 の演算で閉じた (条件 2), 最小の集合である (条件 3). 再帰的定義であることが明白な場合，(3) の文言は省略することが多い．

上のように定義された E は，(2) の逆，つまり $n+2 \in E$ ならば $n \in E$ を満たす．なぜなら，$n \in E$ でなければ，$n+2$ を E に入れる必要はなく，必要ないものは入れないというのが (3) の主張だから，$n+2 \in E$ でない．したがって，(2) の条件は

(2′) $n \in E \Leftrightarrow n+2 \in E$

と表してもよい．

われわれがよく用いる再帰的定義の典型例として，ある算術の形式体系における「項」の定義を考えてみよう：

(1) 変数 $x_0, x_1, \cdots$ と定数 $c_0, c_1, \cdots$ はすべて項である．

(2) s と t が項であれば，$(s)+(t)$ と $(s)\cdot(t)$ は項である．

この定義のもとで，たとえば，$((x_0)\cdot((x_1)+(c_1)))\cdot(c_0)$ は項である．実際には，カッコを適当に省略して，この項を $(x_0\cdot(x_1+c_1))\cdot c_0$ などと表すことになる．

さて，こうして再帰的に定義されたものに関して，それが何らかの性質をもつことを示す際に用いられる有力な手段が**帰納法**である．なかでも，自然数に関する性質を証明する際に用いられる帰納法は，**数学的帰納法**と呼ばれる．上で非負偶数の集合 E を再帰的に定義したが，その定義の +2 を +1 に置き換えたものが，自然数全体の集合 $\mathbf{N}$ の定義に他ならない．すべての自然数 n が性質 $P(n)$ を満たすことを証明する場合，数学的帰納法では

(1) $P(0)$ が成り立つ

(2) $P(n)$ が成り立てば，$P(n+1)$ が成り立つ

を示せばよい．性質 P を満たす自然数の集合 $\{n \in \mathbf{N} : P(n)\}$ を考えると，これは 0 を含み，+1 に関して閉じているから，$\mathbf{N}$ の最小性 (条件 3) より，$\mathbf{N}$ と一致する．つまり，すべての自然数 n が性質 $P(n)$ を満たすことになる．

上で定義した「項」に関する簡単な事実として，すべての項は左カッコ “(” と

右カッコ “)” を同数個含むことを証明してみよう．

(1) 変数 $x_0, x_1, \cdots$ と定数 $c_0, c_1, \cdots$ については，カッコがないので明らか．

(2) 項 s が “(” と “)” を m 個ずつ，項 t が “(” と “)” を n 個ずつ含むとしよう．このとき，項 $(s)+(t)$ は “(” と “)” を $m+n+2$ 個ずつ含み，$(s)\cdot(t)$ も同様である．

このことから，すべての項は “(” と “)” を同数個含むことがいえる．なぜなら，“(” と “)” を同数個含む項の集合は，すべての変数と定数を含み，$(s)+(t)$ と $(s)\cdot(t)$ に関して閉じているから，限定条件によって項全体に一致する．

再帰的定義と帰納法による証明は，数学基礎論や計算機科学における議論のもっとも基本的な形態である．他の概念に依存せずに何かを新しく定義しようとした場合，自らを参照しない限りあまり有意義なものは生まれないからであろう．この本でもこの論法は頻繁に現れるので，ここで完全に理解できなくても，先を読み進むうちにすぐに慣れてしまうだろう．

第 2 講　命題論理

2.1　トートロジー

数学の議論には，次の 6 つの論理記号があれば十分であると前講で述べた:

$\neg$ (…でない)，　$\wedge$ (かつ)，　$\vee$ (または)，　$\rightarrow$ (ならば)，

$\forall$ (任意の__について)，　$\exists$ (ある__について).

最初の 4 つの記号を**命題結合記号**，残りの 2 つを**量化記号 (quantifier)** という．この講では，命題結合記号だけを扱う論理体系，いわゆる**命題論理**，について学ぶ．命題論理では「命題」を元素として命題間の論理関係を扱うのだが，量化記号を使って原子命題をさらに (主語)＋(述語) のように分解して調べるのが**述語論理**である．それについては次講で述べる．

定義．$p_0, p_1, p_2, \cdots$ を**原子命題**とする．

原子命題が具体的に何を記述しているのかは以下の議論では重要でない．たとえば，$p_0 =$「$1+1=2$」, $p_1 =$「ソクラテスはギリシャ人だ」，$p_3 =$「この本の著者は宇宙人だ」などと置いてもよい．常識的な解釈においてこの p_0 は真になるが，それがいつも真であるという論理的根拠はない．p_0 の文構造を分析し，それがある種の数学的な公理から導かれるというようなことは述語論理の話である．ここでは，すべての原子命題は，それぞれ独立に真にも偽になるものとしておこう．

一般の命題は，原子命題を命題結合記号でつないで作られる．正確には次のように定義する．

定義．**命題**は，次のように再帰的に定義される：

(1) 原子命題は命題である．

(2) A と B が命題であれば，$\neg(A)$, $(A)\wedge(B)$, $(A)\vee(B)$ および $(A)\rightarrow(B)$ はそれぞれ命題である．

たとえば，$(\neg(p_1)) \wedge ((p_3) \to ((p_1) \vee (p_2)))$ は命題である．しかし，今後は誤読が生じない程度に適当にカッコを省略し，$\neg p_1 \wedge (p_3 \to (p_1 \vee p_2))$ などと書くことにする．

原子命題の真偽は自由に選択できても，一般の命題の真偽はそうではない．たとえば，$A \vee \neg A$ は，A の真偽によらずつねに真である．これについて，もう少し詳しく議論していこう．命題 A が真のときその命題は真理値 **T** (true の意) をもつといい，そうでないとき，つまり A が偽のときその命題は真理値 **F** (false の意) をもつという．原子命題については真理値 **T**, **F** を自由に割り当てられると約束したが，原子命題の真理値が定まると一般の命題の真理値は一意に決まるのである．

補題 2.1 原子命題に真理値を割り当てる関数 v は，以下の条件のもとですべての命題に真理値を割り当てる関数 V に一意に拡張できる:

(1) A が原子命題のとき，$V(A) = v(A)$,

(2a) $V(\neg A) = \mathbf{T} \Leftrightarrow V(A) = \mathbf{F}$,

(2b) $V(A \wedge B) = \mathbf{T} \Leftrightarrow V(A) = \mathbf{T}$ かつ $V(B) = \mathbf{T}$,

(2c) $V(A \vee B) = \mathbf{T} \Leftrightarrow V(A) = \mathbf{T}$ または $V(B) = \mathbf{T}$,

(2d) $V(A \to B) = \mathbf{T} \Leftrightarrow V(A) = \mathbf{F}$ または $V(B) = \mathbf{T}$.

補題における関数 V の存在およびその一意性は,「命題」の定義に基づく帰納法で容易に証明できる．このような関数 V を**真理値関数 (truth-value function)** と呼ぶ．

定義. 命題 A がどんな真理値関数 V に対しても $V(A) = \mathbf{T}$ となる場合，そのような命題 A を**トートロジー (tautology)** または**恒真命題**といい，A がトートロジーであることを $\models A$ と書く．

例. 任意の命題 A, B について，$A \to (B \to A)$ はトートロジーである．なぜな

ら，もしもある真理値関数 V に対して $V(A \to (B \to A)) = \mathbf{F}$ だとすると，上の条件 (2d) より，$V(A) = \mathbf{T}$ かつ $V(B \to A) = \mathbf{F}$ である．いま $V(B \to A) = \mathbf{F}$ に対して再び条件 (2d) を適用すれば，$V(B) = \mathbf{T}$ かつ $V(A) = \mathbf{F}$ となるが，$V(A)$ が同時に $\mathbf{T}$ かつ $\mathbf{F}$ となることはあり得ないので，矛盾である．

問題．次を証明せよ．

(1) $\models (A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(2) $\models (\neg B \to \neg A) \to (A \to B)$

さて，次の目標はトートロジー全体がどんな構造をもっているかを調べることである．その際，4 つの論理記号を一度に全部あつかう必要はない．普通は，$\to$ を省略するか，$\wedge$ と $\vee$ の両方を省略することが多い．前の講でも述べたように，省略した記号を他の記号で定義できるからである．$\to$ を省略する場合，さらに $\wedge$ か $\vee$ の一方を消すことが可能だが，それはシステムの記述をかえってむずかしくするのであまり行われない．$\neg, \wedge, \vee$ (および $\forall, \exists$) の公理系として，本書のパート C にいわゆるゲンツェン (G. Gentzen) 流のものが登場する．本講では $\neg, \to$ だけを扱ういわゆるヒルベルト流の公理系を導入し，それがすべてのトートロジーを生成するという事実 (命題論理の完全性定理) を証明する．ゲンツェン流は推論規則を主とした形式体系で，反対にヒルベルト流は推論規則を少なく，公理を多くした体系である．両者の違いは，下の公理系とパート C のそれを比較していただけば明白であろう．

2.2　命題論理の公理系

ここで扱うのはウカシェビッチ (Łukasziewic) の公理系と呼ばれるもので，公理はたった 3 つ．じつは，すべて上の例や練習問題で用いたものである．名前を付けて，もう一度書いておく．

P1. $A \to (B \to A)$

P2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

P3. $(\neg B \to \neg A) \to (A \to B)$

上式で A, B, C は任意の命題を表すから，正確にいえば，P1, P2, P3 は 3 つの形の命題の集まり (3 つの公理図式) である．以下，公理図式を単に公理と呼ぶ．

これらの公理がトートロジーであることは，すでに見た通りである．これらをもとに別のトートロジーを生成する規則として，**三段論法** (**modus ponens**，あるいはカットとも呼ばれる) を考える．公理から妥当な推論で導出される命題を一般に「定理」と呼ぶが，ここでは次のように「定理」の定義を与える．

定義. 命題論理の**定理**は次のように定義される．

(1) 公理 P1, P2, P3 は定理である．

(2) A と $A \to B$ が定理なら，B も定理である． (三段論法)

この定義も一応は再帰的だが,「命題」の定義などとは少し様子が違っていることに注意しておこう．実際，与えられた文字列が「命題」になるか否かはその文字列の内部を観察すれば判定できるが，与えられた命題が定理になっているか否かは命題の構造を見ただけでは容易に判定できないのである．たとえば，$p_0 \to p_0$ が命題であることは一見して分かるが，それが定理になることは一目では分からない．また逆に，ある命題が定理にならないことは，どうしたら分かるだろうか？このような疑問は，“定理＝トートロジー” という完全性定理を証明することで解決する．なぜなら，ある命題がトートロジーであるか否かは命題の内部構造の観察で判定できるからである．

ここで,「定理」より扱いやすい概念として，定理の生成プロセス，つまり「証明」という概念を導入する．

定義. 命題の列 $A_0, A_1, \cdots, A_n$ が以下の条件を満たしているとき，その列を A_n の**証明**という：各 $k \leq n$ について，

(1) A_k は公理 (P1, P2, P3) であるか，

(2) $i, j < k$ が存在して A_j は $A_i \to A_k$ である．(A_k は，A_i と A_j から三段論法によって導かれる．)

例．次の命題の列 A_0, A_1, A_2, A_3, A_4 は，$A \to A$ の証明である．

$A_0 = A \to ((A \to A) \to A)$: P1

$A_1 = (A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$: P2

$A_2 = (A \to (A \to A)) \to (A \to A)$: $A_1 = A_0 \to A_2$

$A_3 = A \to (A \to A)$: P1

$A_4 = A \to A$: $A_2 = A_3 \to A_4$

問題．(各 30 分以内で解ければ有段者)

(1) $\neg A \to (A \to B)$ の証明を求めよ．

(2) $\neg\neg A \to A$ の証明を求めよ．

ヒント (上級者見るべからず)：(1) まず，命題 D が定理ならば，任意の命題 C に対し，$C \to D$ も定理になることを P1 (および三段論法) を使って示せ．これにより，$\neg A \to ((\neg B \to \neg A)) \to (A \to B))$ は定理である．これから，P1 と P2 を使って，$\neg A \to (A \to B)$ が得られる．(2) 問題 (1) において，A に $\neg A$ を，B に $\neg\neg\neg A$ を代入し，その結果に対し P2, P3 を適当に使えば，$\neg\neg A \to (\neg\neg A \to A)$ が得られる．再び P2 を使い，また上の例から $\neg\neg A \to \neg\neg A$ がいえるので，$\neg\neg A \to A$ となる．

ここで，どんな「定理」も必ず「証明」をもつことを示しておこう．「証明」をもつ命題全体は，すべての公理を含み，三段論法に関して閉じている．「定理」全体の集合は，そのような性質を持つ最小の集合として定義されるのだから，「証明」をもつ命題全体の集合の部分集合になる．つまり，どんな「定理」も「証明」をもつ．逆に，「証明」をもつ命題が「定理」になることは明らかである．

次に，証明の概念を少し拡張する．

定義．命題の集合 Σ が与えられたとき，以下の条件を満たす命題の列 $B_0, B_1, \cdots$, B_n を Σ における B_n の証明という：各 $k \leqq n$ について，

(1) B_k は公理であるか，Σ に属するか，

(2) $i, j < k$ が存在して $B_j = B_i \to B_k$ となる．

Σ における B の証明が存在するとき，B は Σ で**証明可能**であるといい，$\Sigma \vdash B$ と書く．$\Sigma = \emptyset$ のときは，単に $\vdash B$ と書く．

定理 2.2 (演繹定理) $\Sigma \cup \{A\} \vdash B$ ならば，$\Sigma \vdash A \to B$.

[証明]　$\Sigma \cup \{A\}$ における B の証明を $B_0, B_1, \cdots, B_k (= B)$ とし，証明の長さ $k+1$ に関する帰納法で証明する．最初に，$k = 0$ の場合を考える．

(1) B が公理または Σ に属するとき，

$A_0 = B$ ：公理または Σ に属する

$A_1 = B \to (A \to B)$ ：P1

$A_2 = A \to B$ ：$A_1 = A_0 \to A_2$

は，Σ における $A \to B$ の証明である．

(2) $B = A$ のとき，$A \to B$ は $A \to A$ と同じだから，上の例に示した通り証明可能．

次に，k > 1 の場合．

(1) $B_k = B$ が公理か，$\Sigma \cup \{A\}$ の要素のとき．上の場合と同様．

(2) $i, j < k$ が存在して $B_j = B_i \to B_k$ とき．帰納法の仮定から，$\Sigma \vdash A \to B_i$ および $\Sigma \vdash A \to B_j$ がいえる．いま，$A_0, A_1, \cdots, A_m$ を Σ における $A \to B_i$ の証明とし，$A_{m+1}, \cdots, A_n$ を Σ における $A \to B_j$ の証明とする．すると，$A_0, \cdots, A_m, A_{m+1}, \cdots, A_n$ は Σ における $A \to B_j$ の証明である．そして，以下の A_{n+1}, A_{n+2}, A_{n+3} を $A_0, \cdots, A_n$ のあとに付け加えれば，Σ における $A \to B$ の証明を得る．

$A_{n+1} = (A \to (B_i \to B_k)) \to ((A \to B_i) \to (A \to B_k))$ ：P2

$A_{n+2} = (A \to B_i) \to (A \to B_k)$ ：$A_{n+1} = A_n \to A_{n+2}$

$$A_{n+3} = A \to B_k \qquad : A_{n+2} = A_m \to A_{n+3}$$

□

演繹定理の逆，すなわち $\Sigma \vdash A \to B$ ならば $\Sigma \cup \{A\} \vdash B$, は三段論法によってただちに得られる．演繹定理の有用性は，次の例題だけでも納得できよう．

例題． $\vdash \neg A \to (A \to B)$ を示せ．
演繹定理により，$\{\neg A, A\} \vdash B$ をいえばよい．$\{\neg A, A\} \vdash \neg A$ だから，P1 および三段論法を使って $\{\neg A, A\} \vdash \neg B \to \neg A$. $P3$ より $\{\neg A, A\} \vdash A \to B$. 三段論法で，$\{\neg A, A\} \vdash B$. □

この例は，矛盾 ($\neg A$ かつ A) から任意の命題 B が導けることを意味する．これを少し詳しく見ていこう．まず,「矛盾」を表す命題 $\perp$ を $\neg(p_0 \to p_0)$ と定める．

定義. 命題の集合 Σ から $\perp$ が証明されるとき，Σ は**矛盾する**という．そうでないとき，Σ は**無矛盾**であるという．

次の 2 つの補題は，上の例題を用いれば容易に証明できる．(問題 : 証明せよ．)

補題 2.3　Σ が矛盾するとき，任意の命題 B に対して，$\Sigma \vdash B$.

補題 2.4　$\Sigma \vdash A$ かつ $\Sigma \vdash \neg A$ となる命題 A があれば，Σ は矛盾している．言い換えると，Σ が無矛盾であれば，任意の A に対し，A か $\neg A$ の少なくとも一方は Σ で証明できない．

次の補題は，証明可能性と矛盾の概念を結ぶ基本原理である．

補題 2.5　$\Sigma \cup \{\neg A\}$ が矛盾する　$\Leftrightarrow$　$\Sigma \vdash A$.

[証明] $\Rightarrow$ の証明. $\Sigma\cup\{\neg A\}\vdash\neg(p_0\to p_0)$ とすると，演繹定理により，$\Sigma\vdash\neg A\to\neg(p_0\to p_0)$. したがって，P3 から，$\Sigma\vdash(p_0\to p_0)\to A$. $\vdash(p_0\to p_0)$ より，$\Sigma\vdash A$.

$\Leftarrow$ の証明. $\Sigma\vdash A$ ならば，$\Sigma\cup\{\neg A\}$ からは A と $\neg A$ が両方証明できるので，矛盾する. □

次の補題は，完全性定理の証明の要になるものである.

補題 2.6 Σ が無矛盾であれば，任意の A に対し，$\Sigma\cup\{A\}$ か $\Sigma\cup\{\neg A\}$ の少なくとも一方は無矛盾である.

[証明] 補題 2.4 および 2.5 による. □

2.3 命題論理の完全性定理

定理 2.7 (命題論理の完全性定理) $\vdash A\ \Leftrightarrow\ \models A$

[証明] $\Rightarrow$ の証明. V を任意の真理値関数とする. 3 つの公理 A について，$V(A)=\mathbf{T}$ となることはすでに見た. また，$V(A)=\mathbf{T}$ かつ $V(A\to B)=\mathbf{T}$ のとき，$V(B)=\mathbf{T}$ となることも容易にわかる. よって，すべての定理 A について，$V(A)=\mathbf{T}$ となる.

$\Leftarrow$ の証明. 命題 A が定理でないとし，それに値 $\mathbf{F}$ を割り当てる真理値関数が存在することをいえばよい. まず，すべての命題を適当な順番に並べて，$A_0,A_1,A_2,\cdots$ とする. (注：記号の集合は可算だから，(有限長の) 記号列全体も可算になる. あるいは，すべての命題にゲーデル数 (パート B 参照) を割り当て，それによって並べることも可能.) $\Sigma_0=\{\neg A\}$ とおき (これは補題 2.5 により無矛盾)，無矛盾な集合の無限増加列 $\Sigma_0\subsetneqq\Sigma_1\subsetneqq\Sigma_2\subsetneqq\cdots$ を以下のように定める. 任意の $n\geq 0$ に対して，$\Sigma_n\cup\{A_n\}$ が無矛盾なら，$\Sigma_{n+1}=\Sigma_n\cup\{A_n\}$ とおき，そうでないときは $\Sigma_{n+1}=\Sigma_n$ とおく.

すると，$\Sigma=\bigcup_n\Sigma_n$ は無矛盾である. なぜなら，もしも Σ から矛盾 $\bot$ が導か

れるなら，その証明に用いられる Σ の要素は有限個だから，十分大きな n に対して，それらはすべて Σ_n に入る．したがって，$\Sigma_n \vdash \perp$ となるが，これは Σ_n の無矛盾性に反する．また Σ は極大な無矛盾集合になっている．すなわち，任意の論理式 A_n に対し，$A_n \in \Sigma$ または $\neg A_n \in \Sigma$ がいえる．いま，$\Sigma \not\vdash A_n$ とすると，$\Sigma \cup \{\neg A_n\}$ は無矛盾だから，$A_m = \neg A_n$ として，$A_m \in \Sigma_{m+1} \subsetneqq \Sigma$ である．つまり，$\Sigma \not\vdash A_n$ ならば，$\neg A_n \in \Sigma$ である．同様にして，$\Sigma \not\vdash \neg A_n$ ならば，$A_n \in \Sigma$ もいえる．Σ は無矛盾だから，補題 2.4 より A_n か $\neg A_n$ のどちらかが Σ に属することがわかる．このとき，任意の論理式 A_n に対し，$A_n \notin \Sigma \Leftrightarrow \neg A_n \in \Sigma$ となることも注意しておく．

さてそこで，次のように関数 V を定義する：

$$V(A_n) = \mathbf{T} \Leftrightarrow A_n \in \Sigma_{n+1}.$$

この定義から，最初に選んだ A ($\Sigma_0 = \{\neg A\}$) に対して $V(A) = \mathbf{F}$ は明らかなので，あとはこの関数 V が真理値関数であることをいえばよい．まず，

$$V(\neg A_n) = \mathbf{T} \Leftrightarrow V(A_n) = \mathbf{F}$$

であることは，上の段落で述べた極大無矛盾性よりただちにいえる．また，

$$V(A_m \to A_n) = \mathbf{T} \Leftrightarrow V(A_m) = \mathbf{F} \text{ または } V(A_n) = \mathbf{T}$$

となることも，極大無矛盾性によって

$$A_m \to A_n \in \Sigma \Leftrightarrow \neg A_m \in \Sigma \text{ または } A_n \in \Sigma$$

が簡単に示せるので問題ない．よって，V は命題 A に値 $\mathbf{F}$ を割り当てる真理値関数であり，A はトートロジーでない．□

証明可能性 $\vdash$ を一般化したように，恒真性 $\models$ も一般化できる．すなわち，Σ の命題すべてに値 $\mathbf{T}$ を割り当てる任意の真理値関数が命題 A に値 $\mathbf{T}$ を割り当てるとき，$\Sigma \models A$ と書き，A は Σ のトートロジー的帰結であるという．そして，完全性定理も次のように一般化できる．

定理 2.8 (命題論理の一般化された完全性定理) $\Sigma \vdash A \Leftrightarrow \Sigma \models A.$

[証明] $\Rightarrow$ の証明．V を Σ のすべての命題に値 $\mathbf{T}$ を割り当てる真理値関数とす

る．3 つの公理 A については，すでに見たように $V(A)=\mathbf{T}$. また，$V(A)=\mathbf{T}$ かつ $V(A\to B)=\mathbf{T}$ のとき，$V(B)=\mathbf{T}$. よって，Σ から導かれるすべての定理 A について，$V(A)=\mathbf{T}$ となる．

$\Leftarrow$ の証明．命題 A が Σ の定理でないとし，それに値 $\mathbf{F}$ を割り当て，Σ の命題すべてに値 $\mathbf{T}$ を割り当てる真理値関数が存在することをいえばよい．定理 2.7 の証明において，$\Sigma_0=\Sigma\cup\{\neg A\}$ と置き直すだけでよい．□

定理 2.9 (命題論理のコンパクト性定理) Σ の任意の有限部分集合に対し，それに属するすべての命題に値 $\mathbf{T}$ を割り当てる真理値関数が存在すれば，Σ の命題すべてに値 $\mathbf{T}$ を割り当てる真理値関数が存在する．

[証明] 対偶を示す．Σ の命題すべてに値 $\mathbf{T}$ を割り当てる真理値関数は存在しないと仮定する．証明すべきことは，Σ のある有限部分集合があって，それに属するすべての命題に値 $\mathbf{T}$ を割り当てる真理値関数が存在しないことである．さて，この仮定のもとでは，どんな命題も Σ のトートロジー的帰結になるが，特に $\Sigma\models\neg(p_0\to p_0)$ である．したがって，一般化された完全性定理により $\Sigma\vdash\neg(p_0\to p_0)$ を得る．証明は有限個の命題で構成されているので，Σ のある有限集合 Σ' が存在して，$\Sigma'\vdash\neg(p_0\to p_0)$. 再び，一般化された完全性定理により $\Sigma'\models\neg(p_0\to p_0)$. $\neg(p_0\to p_0)$ に値 $\mathbf{T}$ を割り当てる真理値関数は存在しないので，Σ' の命題すべてに値 $\mathbf{T}$ を割り当てる真理値関数も存在しない．□

この定理の名称は，ハイネ (H. Heine)–ボレル (A. Borel) の意味での位相空間のコンパクト性に由来する．それを明らかにするために別証を付けておこう．位相空間の議論に不慣れな読者はここを飛ばしてよい．

[別証]　$X=\{\mathbf{T},\mathbf{F}\}^{\mathbf{N}}$ を直積位相を伴う位相空間と考える．ただし，$\{\mathbf{T},\mathbf{F}\}$ には離散位相が入っているものとし，有限空間は必ずコンパクトなので，チコノフ (A. Tychonoff, Tikhonov) の定理によりその直積空間 X もコンパクトになっている．X の元は，原子命題 $p_0,p_1,p_2,\cdots$ に真理値 $\mathbf{T}$, $\mathbf{F}$ を割り当てる関数 v と解釈

できる．また，関数 v は一意に真理値関数 $V = \bar{v}$ に拡張できるので，それらは同一視してもよい．さて，命題 A に対し，それに真理値 $\mathbf{T}$ を割り当てる関数 v 全体を C_A とおく．すなわち，$C_A = \{v \in X : \bar{v}(A) = \mathbf{T}\}$. ここで，$A$ に含まれる原子命題が有限個しかないことから，C_A は X の開閉 (clopen) 集合である．実際，C_A は $B_i = \{v \in X : v(i) = \mathbf{T}\}$ の形の開閉集合から有限ブール (G. Boole) 演算で得られる．

さて，Σ の命題すべてに値 $\mathbf{T}$ を割り当てる真理値関数が存在するということは，$\bigcap\{C_A : A \in \Sigma\} \neq \emptyset$ で表現できる．したがって，命題論理のコンパクト性定理は，Σ の任意の有限部分集合 Σ' に対して $\bigcap\{C_A : A \in \Sigma'\} \neq \emptyset$ ならば，$\bigcap\{C_A : A \in \Sigma\} \neq \emptyset$ という主張になるが，これは位相空間 X がコンパクトであるという主張に他ならない．□

第 3 講　述語論理

3.1　構造と言語

述語論理における命題は数学的構造についての記述である．この節の目標は，ある種の構造の集まり (たとえば，群全体) に対し，共通して成り立つ命題がどのようなものかを調べることである．まず構造の定義から始めよう．

定義． **構造** $\mathfrak{A} = (A, F, R)$ は次のものからなる：

(1) A は空でない集合で，構造 $\mathfrak{A}$ の**領域** (または宇宙) と呼ばれる．$A = |\mathfrak{A}|$ と記す．

(2) $F = \{f_i : i \in I\}$ は A 上の関数 (演算) の集まりである．

(3) $R = \{R_j : j \in J\}$ は A 上の関係 (述語) の集まりである．

ここで，A 上の関数 f とは，ある n に対して $f : A^n \to A$ となる n 変数関数で，n を f の元数 (**arity**) という．とくに，元数 0 の関数を定数 (**constant**) と呼び，それをその値 $a \in A$ と同一視する．A 上の n 項関係 R は A^n の部分集合であり，n を R の元数 (**arity**) という．元数 0 の関係は，真理値定数 **T** または **F** と見なすことができる．

記法の簡便さと直感的理解のため，F や R が非可算集合のときも含めて，$F = \{f_0, f_1, \cdots\}$, $R = \{R_0, R_1, \cdots\}$ と書き，構造を

$$\mathfrak{A} = (A; f_0, f_1, \cdots; R_0, R_1, \cdots)$$

で表す．また，誤読が生じない限り，仕切り記号としてセミコロン; の代わりにコンマ, を用いる．各 f_i の元数を m_i とし，各 R_j の元数を n_j とするとき，

$$\rho = (m_0, m_1, \cdots; n_0, n_1, \cdots)$$

を構造 $\mathfrak{A}$ の**類型** (**similarity type**) という．

例．$\mathbf{Z}$ を整数の集合，$0, 1$ を $\mathbf{Z}$ の元，$+, \cdot$ を $\mathbf{Z}$ 上の和積演算，$\leqq$ を大小関係とすると，$\mathfrak{Z} = (\mathbf{Z}; 0, 1, +, \cdot; \leqq)$ または $(\mathbf{Z}, 0, 1, +, \cdot, \leqq)$ は，類型 $\rho = (0, 0, 2, 2; 2)$ の構造である．

上の例について，少し注意して見てみよう．ここでは，$+$ を $\mathbf{Z}$ 上の和算としてあるが，それは $\mathbf{Z}$ 上の和算を記号 $+$ で指し示すということである．構造にとっては，指し示された関数自体に意味があるのであって，どんな記号でそれを示すかは言語の問題である．しかし，言葉なしには何の議論もできないので，構造を導入する際には，その類型 ρ に相応する記号の列 (上の例ならば，元数 0, 0, 2, 2 のそれぞれの関数記号と元数 2 の関係記号) も一緒に与えるのが普通である．そのような記号列を類型 ρ の言語と呼ぶ．大切なことなので，きちんと定義しておこう．

定義．各 f_i を元数 m_i の関数記号，各 R_j を元数 n_j の関係記号とするとき，

$$L = (f_0, f_1, \cdots; R_0, R_1, \cdots)$$

を類型 $\rho = (m_0, m_1, \cdots; n_0, n_1, \cdots)$ の言語という．

言語 L における構造，あるいは単に L-構造という言い方をするとき，それは言語 L による表現を伴った構造という意味である．このとき，構造と言語は同じ類型をもち，言語 L の各記号が指し示す関数や関係は自明に定まっていると考える．関数記号 f が指し示す構造 $\mathfrak{A}$ の関数は $f^{\mathfrak{A}}$ などと記すことが多い．しかし，記号とそれが指し示すものを表記法で完全に区別することは記述をひどく複雑にすることがあるので，その区別が議論の本質に関わらないときはあえて両者を混同して用いることにする．

言語 L の関数記号を合成してできる記号列を L の項という．正確な定義は以下の通り．

定義．言語 L の項は次のように定義される：

(1) 変数記号 $x_0, x_1, x_2, \cdots$ は，言語 L の項である．

(2) f を L の m 変数関数記号とし，$t_0, t_1, \cdots, t_{m-1}$ を L の項とするとき，$f(t_0, t_1, \cdots, t_{m-1})$ は L の項である．

(2) から，L の定数記号 (0 変数関数) はすべて項になる．項 t に含まれるいくつかの変数記号 (たとえば x, y) に注目して，$t(x, y)$ のように記すことがある．項 $t(x)$ に現れる変数記号 x をすべて項 s に置き換えてできる項を $t(s)$ のように表す．また，慣習にしたがって，2 変数関数 $f(x, y)$ は xfy のようにも表す．たとえば，$+(x, y)$ を $x + y$ と書く．

変数を含まない項については，構造における値が一意に定まる．

定義．$\mathfrak{A}$ を言語 L における構造とする．変数を含まない L の項 t に対し，$\mathfrak{A}$ におけるその値 $t^{\mathfrak{A}}$ を以下のように定める：

m 変数関数記号 f に対応する $\mathfrak{A}$ の関数を $f^{\mathfrak{A}}$ とし，項 $t_0, t_1, \cdots, t_{m-1}$ の値を $t_0^{\mathfrak{A}}, t_1^{\mathfrak{A}}, \cdots, t_{m-1}^{\mathfrak{A}}$ とするとき，項 $f(t_0, t_1, \cdots, t_{m-1})$ の値は $f^{\mathfrak{A}}(t_0^{\mathfrak{A}}, t_1^{\mathfrak{A}}, \cdots, t_{m-1}^{\mathfrak{A}})$ によって定まる $|\mathfrak{A}|$ の要素である．

定義．言語 L の原子式は次のように定義される記号列である：

(1) 言語 L の項 s, t に対し，$s = t$ は L の原子式である．

(2) R を L の n 項関係記号とし，$t_0, t_1, \cdots, t_{n-1}$ を L の項とするとき，$R(t_0, t_1, \cdots, t_{n-1})$ は L の原子式である．

変数を含まない原子式に対する真偽の概念を次のように定める．

定義．$\mathfrak{A}$ を言語 L における構造とする．

(1) 変数を含まない項 s, t に対し，$s^{\mathfrak{A}}$ と $t^{\mathfrak{A}}$ が同じ値であれば，原子式 $s = t$ は $\mathfrak{A}$ において真であり，そうでなければ偽であるという．

(2) R を L の n 項関係記号とし，$t_0, \cdots, t_{n-1}$ を L の項として，$R^{\mathfrak{A}}(t_0^{\mathfrak{A}}, \cdots, t_{n-1}^{\mathfrak{A}})$ が成り立つならば，原子式 $R(t_0, \cdots, t_{n-1})$ は $\mathfrak{A}$ において**真**であり，そうでなければ**偽**であるという．

定義．言語 L の**論理式**は次のように再帰的に定義される：

(1) 言語 L の原子式は，言語 L の論理式である．

(2) φ と ψ を言語 L の論理式，x を変数記号として，$\neg(\varphi), (\varphi) \wedge (\psi), (\varphi) \vee (\psi), (\varphi) \to (\psi), \forall x(\varphi), \exists x(\varphi)$ は言語 L の論理式である．

命題論理の命題と同様，論理式のカッコは適当に省略して表す．たとえば，$\varphi_1, \varphi_2, \varphi_3$ を原子式として，$\exists y\, \varphi_1 \vee \forall x(\varphi_2 \to \exists y\, \varphi_3)$ は論理式である．論理式 ψ を構成する過程で現れる論理式を ψ の**部分式**と呼ぶ．$\psi = \exists y\, \varphi_1 \vee \forall x(\varphi_2 \to \exists y \varphi_3)$ の部分式は，3つの原子式 $\varphi_1, \varphi_2, \varphi_3$ と ψ 自身の他に，$\exists y\, \varphi_1, \exists y\, \varphi_3, \varphi_2 \to \exists y\, \varphi_3, \forall x(\varphi_2 \to \exists y\, \varphi_3)$ の4つである．

論理式に含まれる変数記号に別の項を代入する場合は，多少厄介な注意が必要である．変数記号には，論理式のなかで量化記号 $\forall, \exists$ によって束縛されているものと，そうでないものがあり，それらの役割はまったく異なるからである．$\forall x\, \varphi(x)$ という式は素朴には「すべての x について，$\varphi(x)$ が成り立つ」という意味であり，したがって束縛変数 x を別の (新しい) 変数 y に置き換えて $\forall y\, \varphi(y)$ としてもその意味は変わらない．$\forall x\, \varphi(x)$ を部分式として含む論理式についても，その箇所だけで変数 x を別の変数に置き換えることが可能である．しかし，他の形の部分式に対して勝手に変数を置き換えることはできない．極端な話，$\forall x\, \varphi(x)$ の $\varphi(x)$ の部分だけに $x = y$ を代入すれば $\forall x\, \varphi(y)$ が得られるが，これではもとの式と意味が変わってしまう．

いま，式 (または部分式) $\forall x\, \varphi(x, z)$ の変数 z に項 t を代入することを考える．このとき，もし項 t が変数 x を含んでいると，代入の結果その変数 x は $\forall x$ によって束縛されるが，これは望ましくない．というのは，上に述べたように $\forall x\, \varphi(x, z)$ における束縛変数 x は置き換え自由だから，$\forall x\, \varphi(x, z)$ へ $z = t$ を代入した結果

が $\forall y\,\varphi(y,z)$ に同じものを代入した結果と意味が変わっては困る．そこで，次のような約束をしておく．代入項に含まれる変数が代入の結果束縛されてしまう場合，束縛変数の方を予め新しい変数に置き換えておく．つまり，$\forall x\,\varphi(x,z)$ に $z=t$ を代入する場合，$\varphi(x,z)$ にも t にも含まれない新しい変数を y として，$\forall y\,\varphi(y,t)$ を代入結果とする．

このような約束事は普通無意識に実行されていることだから，わかりにくければあまり気にされる必要はない．逆に，上の説明では束縛変数の定義や置き換え可能性の定義が曖昧だと思われる方は，正確な定義を自分で考えてみてほしい．論理式を扱う計算機プログラムを作ろうとしてみれば，こういうところが結構重要な作業であることがわかる．

さて，以上のもとで，一般の論理式に対する真偽の概念を定義しよう．まず，言語 L および L 構造 $\mathfrak{A}=(A,F,R)$ を固定して議論をすすめる．B を領域 A の部分集合とし，B の各要素 b に対する新しい定数 b^* を L に加えた言語を L_B で表す．すなわち，$L_B = L\cup\{b^* : b\in B\}$．そして，定数 b^* の解釈を b として，構造 $\mathfrak{A}$ を言語 L_B に拡張したものを $\mathfrak{A}_B$ で表す．たとえば，整数順序環 $\mathfrak{Z}=(\mathbf{Z};0,1,+,\cdot;\leq)$ に対して，$\mathfrak{Z}_{\mathbf{N}}=(\mathbf{Z};0,1,+,\cdot,0^*,1^*,2^*,\cdots;\leq)$ である．以下では，$|\mathfrak{A}|$ の要素 a と定数 a^* の区別は厳密にしない．論理式 φ に含まれるすべての変数がそのなかで束縛されているとき，φ を文 (**sentence**) または命題と呼ぶ．構造 $\mathfrak{A}$ における文の真偽の概念は構造 $\mathfrak{A}_A$ を介して定義される．

定義．構造 $\mathfrak{A}_A$ で真となる文全体 $Th(\mathfrak{A}_A)$ を次のように定義する：

- L_A の原子文 φ について，$\varphi\in Th(\mathfrak{A}_A)\Leftrightarrow\varphi$ は $\mathfrak{A}_A$ で真
- $\neg\varphi\in Th(\mathfrak{A}_A)\Leftrightarrow\varphi\notin Th(\mathfrak{A}_A)$
- $\varphi\wedge\psi\in Th(\mathfrak{A}_A)\Leftrightarrow\varphi\in Th(\mathfrak{A}_A)$ かつ $\psi\in Th(\mathfrak{A}_A)$
- $\varphi\vee\psi\in Th(\mathfrak{A}_A)\Leftrightarrow\varphi\in Th(\mathfrak{A}_A)$ または $\psi\in Th(\mathfrak{A}_A)$
- $\varphi\to\psi\in Th(\mathfrak{A}_A)\Leftrightarrow\varphi\in Th(\mathfrak{A}_A)$ でないか $\psi\in Th(\mathfrak{A}_A)$
- $\forall x\varphi(x)\in Th(\mathfrak{A}_A)\Leftrightarrow$ すべての定数 a について，$\varphi(a)\in Th(\mathfrak{A}_A)$
- $\exists x\varphi(x)\in Th(\mathfrak{A}_A)\Leftrightarrow$ ある定数 a が存在し，$\varphi(a)\in Th(\mathfrak{A}_A)$

$Th(\mathfrak{A}_A)$ は構造 $\mathfrak{A}$ の初等ダイヤグラム (**elementary diagram**) と呼ばれる．$Th(\mathfrak{A}_A)$ に含まれる原始文と原始文の否定だけを集めた集合を構造 $\mathfrak{A}$ の基本ダイヤグラム (**basic diagram**) という．

定義．L の文 φ が $Th(\mathfrak{A}_A)$ に属するとき，φ は構造 $\mathfrak{A}$ で真であるといい，$\mathfrak{A} \models \varphi$ と書く．自由変数 $x_0, \cdots, x_{n-1}$ を含む一般の論理式 φ に対しては，$\forall x_0 \cdots \forall x_{n-1}\varphi$ が構造 $\mathfrak{A}$ で真であるときに φ は真であるといい，$\mathfrak{A} \models \varphi$ と書く．

定義．言語 L の文の集合 T が $Th(\mathfrak{A}_A)$ の部分集合になるとき，構造 $\mathfrak{A}$ は理論 T のモデル (**model**) であるといい，$\mathfrak{A} \models T$ と書く．

モデルの存在を議論するとき，しばしば問題になるのは $Th(\mathfrak{A}_A)$ の存在である．そのため，厳密には構造 $\mathfrak{A}$ と $Th(\mathfrak{A}_A)$ の組をモデルと呼ぶべきであろう．一例として，算術のモデルについて考えてみよう．$\mathbf{N}$ をゼロ 0 を含む自然数の集合とし，$+$ と $\cdot$ を $\mathbf{N}$ 上の和積演算，S を後者関数 $(\mathrm{S}(x) = x + 1)$ とする．このとき，次の類型 $(2, 2, 1, 0)$ の構造を算術の標準モデルという：

$$\mathfrak{N} = (\mathbf{N}, +, \cdot, \mathrm{S}, 0).$$

$\mathfrak{N}$ は数学的に自明な構造であり，その存在を問題視するような哲学的議論は本書と無縁である．我々にとって問題になのは $Th(\mathfrak{N}_\mathbf{N})$ であって，これは算術的に定義できない集合であることが知られている (タルスキ (A. Tarski) の定理)．実際，$Th(\mathfrak{N}_\mathbf{N})$ が何かはっきりわからないので，その近似としてペアノ (G. Peano) の算術のような公理系が考案されているのである．

3.2　ゲーデルの完全性定理

言語 L のいくつかの文を公理とする理論 T が与えられたとする．このとき，T のモデルに共通した性質は何であろうか？

定義．T を言語 L の文の集合とし，φ を L の論理式とする．T の任意のモデル

$\mathfrak{A}$ において，$\mathfrak{A} \models \varphi$ となるとき，φ は T の帰結 (**consequence**) であるといい，$T \models \varphi$ と書く．

φ を T に属する文や命題論理のトートロジーの形の文とすれば，明らかに $T \models \varphi$ の関係を満たすが，他にはどのようなものがあるだろうか？ 結論からいえば，$T \models \varphi$ の関係は，命題論理の場合と同様に，形式的公理体系として捕らえることができるというのが，ゲーデルの完全性定理である．

定義. 文の集合 T が与えられたとき，次の条件を満たす L の論理式の列 $\varphi_0, \varphi_1, \cdots, \varphi_n$ を T における φ_n の証明という：各 $k \leqq n$ について，

(1) φ_k は T に属するか，

(2) φ_k は次の公理のどれかか，

P1. $\varphi \to (\psi \to \varphi)$

P2. $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$

P3. $(\neg\psi \to \neg\varphi)) \to (\varphi \to \psi)$

P4. $\forall x\, \varphi(x) \to \varphi(t)$

P5. $x = x$

P6. $x = y \to (\varphi(x) \to \varphi(y))$

(3) $i, j < k$ が存在して $\varphi_j = \varphi_i \to \varphi_k$ となるか，

(4) $i < k$ が存在して $\varphi_i = \psi \to \theta(x)$ かつ $\varphi_k = \psi \to \forall x\, \theta(x)$, ただし x は ψ に現れない．

T において φ の証明が存在するとき，φ は T の定理であるといい，$T \vdash \varphi$ と書く．また $T = \emptyset$ のときは，単に $\vdash \varphi$ と書く．

命題論理との違いは，(2) の P4, P5, P6 および (4) である．P4, P5, P6 の正当性は明らかであろう．(4) は一般化法則 (**generalization**) と呼ばれるもので，前提 ψ と無関係な x について $\theta(x)$ が導かれるならば，ψ から $\forall x\, \theta(x)$ も導かれるという意味である．これから，$T \vdash \theta(x)$ ならば $T \vdash \forall x\, \theta(x)$ となることも容易に

いえる．また，$\wedge, \vee, \exists$ は上の公理系に現れる 3 つの論理記号によって定義すればよいから，それらについての公理は省く．

定理 3.1　言語 L の任意の論理式 φ について，$T \vdash \varphi$ ならば $T \models \varphi$.

[証明]　T における証明の長さに関する帰納法による．□

定理 3.2 (演繹定理)　$T \cup \{\varphi\} \vdash \psi$ ならば，$T \vdash \varphi \to \psi$. ただし，$\varphi$ は文とする．

証明は命題論理の演繹定理とまったく同様である．逆も証明できる．

定義．述語論理において「矛盾」を表す命題 $\perp$ を $\neg\forall x_0(x_0 = x_0)$ と定め，T から $\perp$ が証明されるとき，T は**矛盾する**という．そうでないとき，T は**無矛盾**であるという．

補題 3.3　T が無矛盾であれば，任意の文 φ に対し，$T \cup \{\varphi\}$ か $T \cup \{\neg\varphi\}$ の少なくとも一方は無矛盾である．

証明は命題論理の場合と同様である．

補題 3.4　言語 L の理論 $T \cup \{\neg\forall x\, \neg\varphi(x)\}$ が無矛盾であるとき，L に新しい定数記号 c を加えた言語 $L' = L \cup \{c\}$ において $T \cup \{\varphi(c)\}$ も無矛盾である．(注：この c をヘンキンの定数記号 **(Henkin constant)** という．)

[証明]　$T \cup \{\varphi(c)\}$ が矛盾しているとする．このとき，演繹定理を使って，$T \vdash \neg\varphi(c)$ がいえる．$T \vdash \neg\varphi(c)$ の証明に現れる定数 c を証明に現れない変数 x で置き換えれば，$T \vdash \neg\varphi(x)$ の証明が得られる．したがって，$T \vdash \forall x\, \neg\varphi(x)$, これは $T \cup \{\neg\forall x\, \neg\varphi(x)\}$ が無矛盾である仮定に反する．□

定理 3.5 (ゲーデルの完全性定理)　$T \vdash \varphi \iff T \models \varphi$.

[証明] $\Rightarrow$ はすでに見たので， $\Leftarrow$ を証明すればよい．φ が自由変数 $x_0, \cdots, x_n$ を含むときは，φ の代わりに $\forall x_0 \cdots \forall x_n\, \varphi$ を考えてもよいから，φ は文であると仮定しても一般性を失わない．そこで，$T \vdash \varphi$ でないと仮定すると，$T \cup \{\neg\varphi\}$ は無矛盾である．あとは，これがモデルを持つことを証明すれば，$T \models \varphi$ でないことになり，完全性定理が証明される．

$T \cup \{\neg\varphi\}$ がモデルを持つということは，$T \cup \{\neg\varphi\} \subset Th(\mathfrak{A}_A)$ となる構造 $\mathfrak{A}$ が存在することである．そのためには，$T \cup \{\neg\varphi\} \subset S$ となる言語 $L' = L \cup C$ の文の集合 S で次の条件を満たすものを見つければよい：

(0) C は定数記号の集まりであり，$L \cap C = \emptyset$ としておく．

(1) S は無矛盾である．

(2) 言語 L' における任意の文 φ に対して，$\varphi \in S$ または $\neg\varphi \in S$.

(3) 文 $\exists x\, \varphi(x)$ が S に属するとき，定数 $c \in C$ が存在して $\varphi(c) \in S$. ただし，$\exists x\, \varphi(x)$ は $\neg\forall x\, \neg\varphi(x)$ のことである．

そのような S が見つかったとしよう．まず，(1), (2) によって，S から導かれる文 (定理) はすでに S に属していること，つまり S は述語論理の推論に関して閉じていることに注意しておこう．

集合 C 上に次のように同値関係 $\sim$ を定義する:

$$c \sim d \;\Leftrightarrow\; (c = d) \in S.$$

($\sim$ が同値関係になっていることを各自で確かめよ．) そして，C の同値類 $[c] = \{d : d \sim c\}$ の集まりを A とし，L の関数記号 f に対応する $\mathfrak{A}$ の関数 $f^{\mathfrak{A}}$ を

$$f^{\mathfrak{A}}([c_0], [c_1], \cdots, [c_{m-1}]) = [d] \;\Leftrightarrow\; (f(c_0, c_1, \cdots, c_{m-1}) = d) \in S,$$

L の関係記号 R に対応する $\mathfrak{A}$ の関係 $R^{\mathfrak{A}}$ を

$$R^{\mathfrak{A}}([c_0], [c_1], \cdots, [c_{n-1}]) \;\Leftrightarrow\; R(c_0, c_1, \cdots, c_{n-1}) \in S$$

で定義する．すると，任意の論理式 $\varphi(x_0, x_1, \cdots, x_{n-1})$ に対して，

$$\varphi([c_0], [c_1], \cdots, [c_{n-1}]) \in Th(\mathfrak{A}_A) \;\Leftrightarrow\; \varphi(c_0, c_1, \cdots, c_{n-1}) \in S$$

となることが簡単な帰納法でいえる．いま $T \cup \{\neg\varphi\} \subset S$ であるから，$T \cup \{\neg\varphi\} \subset Th(\mathfrak{A}_A)$ である．したがって，構造 $\mathfrak{A}$ は $T \cup \{\neg\varphi\}$ のモデルになる．

さて，上の条件の (1), (2) を満たすような S を作るのは，命題論理の場合と同

様に，無矛盾な集合を拡大していって極限を取ればよい．(3) および (0) を満たすためには，$\exists x\ \varphi(x)$ が無矛盾な集合に属するとき，新しい定数 c を用意して $\varphi(c)$ をその集合に入れる作業を行えばよい．しかし，この 2 つの作業はある意味で相反するものである．つまり，無矛盾な集合を命題論理の方法で拡大すると $\exists x\ \varphi(x)$ の形の式が新しく入ってくるし，新しい定数 c によって言語を拡張すると極大性が崩れる．そこで，この 2 つの操作を交互に無限回行うことで両条件を同時に満たすものを作る．

まず，$S_0 = T \cup \{\neg\varphi\}$ とおく．L のすべての文を並べて，$\varphi_0, \varphi_1, \cdots, \varphi_n, \cdots$ とする．L が高々可算ならこの列も可算になるが，一般には整列定理 (選択公理と同値) が必要である．命題論理の議論と同じように，無矛盾な集合の無限増加列 $S_0^0 \subset S_0^1 \subset S_0^2 \subset \cdots$ を次のように作る．$S_0^0 = S_0$ とおく．任意の $n \geqq 0$ に対して，$S_0^n \cup \{\varphi_n\}$ が無矛盾なら，$S_0^{n+1} = S_0^n \cup \{\varphi_n\}$ とおき，そうでないときは $S_0^{n+1} = S_0^n$ とおく．そして，$S_1 = \cup S_0^n$ とおけば，S_1 は言語 $L' = L$ に対して (1) と (2) の条件を満たす．

次に，S_1 に含まれるすべての $\exists x\ \varphi(x)$ の形の式に対しそれぞれ新しい定数 c_φ を用意し，そのような定数を集めて C_1 とし，S_1 に $\varphi(c_\varphi)$ をすべて加えたものを S_2 とする．(このとき，L が高々可算なら C_1 も S_1 も可算集合であり，L が非可算の場合 C_1 と S_1 の濃度は L の濃度と等しくなることに注意しておこう．)

さて，この S_2 に対し，上と同じようにして言語 $L \cup C_1$ における極大無矛盾集合 S_3 を作る．次に，S_3 に含まれるすべての $\exists x\ \varphi(x)$ に対しそれぞれ新しい定数 c_φ を用意して，その定数の集合を C_3 とし，S_3 に $\varphi(c_\varphi)$ をすべて加えたものを S_4 とする．以下同様に繰り返して，最後に，$S = \bigcup S_n$, $C = \bigcup C_{2n+1}$ とおく．これが (0) から (3) の条件を満たしていることは容易にわかる．以上で完全性定理の証明が完了した．□

この定理により，たとえば，群全体に共通して成り立つ命題の集合は，群の公理から述語論理の公理と推論規則によって導かれる定理の集合と一致することがわかる．この意味で述語論理の体系は完璧であると主張しているのが，完全性定

理である．

注意：ここでの「完全性」は，不完全性定理における「完全性」とは異なる概念である．与えれた言語における任意の文 φ について，$T \vdash \varphi$ か $T \vdash \neg\varphi$ となる理論 T を (後者の意味で) 完全であるという．そして，自然数論のどんな公理系 (厳密な定義はパート B を参照) も完全にはならないというのが，第一不完全性定理である．

ここで，本書の冒頭に出した問題 (問 1) について考えてみよう．完全性定理の証明で実際に用いられる補題 3.4 の主張は,「理論 $T \cup \{\exists x\, \varphi(x)\}$ が無矛盾である」という前提でなく,「無矛盾な理論 T が $\exists x\, \varphi(x)$ を証明する」で十分である．そして，理論 T が $\exists x\, \varphi(x)$ を証明するなら，$T \vdash \varphi(t)$ となる言語 L の項 t がすでに存在すると考えるのは自然である．そして，もしもそうなら，言語をわざわざ拡張せずに L の項を集めただけでもほしいモデルが作れるように思える．しかし，そうはならないのである．

具体的な例として，証明も反証もできない文 σ をもつある算術の公理系 T を考えよう．いま，T は定数 $0, 1$ を持っているとして，$\varphi(x) \leftrightarrow (x = 0 \wedge \sigma) \vee (x = 1 \wedge \neg\sigma)$ とおく．すると，$T \vdash \varphi(0) \vee \varphi(1)$ だから $T \vdash \exists x\, \varphi(x) \vee \exists x\, \varphi(x)$ つまり $T \vdash \exists x\, \varphi(x)$ となる．しかし，$T \vdash \varphi(t)$ となる項 t はない．もし，そのような項が存在したら，矛盾が生じることを示しておこう．いま，t が存在して，それが変数を含んでいれば，そのすべての変数に適当な定数 (たとえば，0) を代入した結果を t' とすれば，やはり $T \vdash \varphi(t')$ となるから，t は変数を含まないと考えてよい．すると，t は具体的な値をもつが，$T \vdash t = 0$ ならば $T \vdash \sigma$, $T \vdash t = 1$ ならば $T \vdash \neg\sigma$ となり，これらは σ が T から独立であるという前提に反する．他方，$T \vdash t \neq 0 \wedge t \neq 1$ ならば，$T \nvdash \varphi(t)$ となり，これも矛盾である．

この例からも予測できるように次のことはいえる．言語 L における述語論理の公理と推論規則だけから $\exists x\, \varphi(x)$ が証明されるなら，言語 L の有限個の項 $t_0, t_1, \cdots, t_n$ が存在して，$\vdash \varphi(t_0) \vee \varphi(t_1) \vee \cdots \vee \varphi(t_n)$ となる．これをエルブラン (**J. Herbrand**) の定理という．

3.3　完全性定理の応用 1

定理 3.6 (レーベンハイム (L. Löwenheim)-スコーレム (A. Skolem) 下降定理) 言語 L における無矛盾な理論は，高々可算もしくは高々 L と同じ濃度のモデルをもつ．

[証明] 完全性定理の証明において，新しい定数記号の集合 C は可算無限もしくは L と同じ濃度を持つ．これから同値類をとって $\mathfrak{A}$ を作っても，やはり $|\mathfrak{A}|$ は高々可算もしくは L と同じ濃度を持つ．□

この定理によれば，述語論理における実数論や集合論なども可算のモデルをもつ．集合論では，巨大な濃度を持つ非可算集合を扱っているはずなのに，そのモデルが可算であるというのは一見不合理のように思われる (スコーレムのパラドックス)．しかし，可算かどうかは，自然数と 1 対 1 に対応する関数があるかどうかであり，その関数が集合論のモデルの外にあれば，モデル内おいては非可算，外では可算ということがあって不思議はないのである．つまり，スコーレムのパラドックスは，パラドックスというより，濃度の概念の相対性を示した画期的な発見といえる．

定理 3.7 (コンパクト性定理) 理論 T がモデルをもつための必要十分条件は，T の任意の有限部分集合がモデルを持つことである．

[証明] T の任意の有限部分集合がモデルをもてば，任意の有限部分集合は無矛盾であり，よって T 全体からも矛盾が導かれることはない．したがって，完全性定理の証明により，T はモデルをもつ．□

命題論理のコンパクト性は，真理値関数がつくるカントル (G. Cantor) 空間のコンパクト性に対応していた．述語論理の場合も，これと類似の議論でモデル全体がつくる空間 (ストーン (M. Stone) 空間) のコンパクト性に対応している．これは現代モデル論にとって大変重要なアイデアであるが，余白の関係で説明を省く．

定理 3.8 (レーベンハイム-スコーレム-タルスキ上昇定理) 言語 L における理論が無限モデルをもてば，L の濃度以上の任意の濃度のモデルをもつ．

[証明] $\mathfrak{A}$ を言語 L の理論 T_0 の無限モデルとし，κ を L の濃度以上の基数とする．κ 個の新しい定数記号の集合 C を用意して，

$$T = T_0 \cup \{\neg c = d : c \text{ と } d \text{ は } C \text{に属する相異なる 2 つの定数}\}$$

とおく．すると，T の任意の有限部分集合 T' はモデル $\mathfrak{A}'$ をもつ．実際，$\mathfrak{A}'$ は $\mathfrak{A}$ に C の定数記号の解釈を適当に加えて，T' に含まれる有限個の式 $\neg c = d$ が成り立つようにするだけでよい．よって，コンパクト性定理から，T 全体がモデルをもつことになるが，T の性質からどのモデルの濃度も κ 以上になる．他方，下降定理により，T は濃度 κ 以下のモデルをもつので，結局ちょうど濃度 κ のモデルが存在することになる．□

この定理により，どんな自然数の公理系にも ($Th(\mathfrak{N}_\mathbf{N})$ でも) 無矛盾である限り非可算モデルが存在することになる．

3.4 完全性定理の応用 2

さらに完全性定理の実際的な応用として，言語とモデルの拡張について考える．最初に，構造の定義を復習しておくと，言語 L における構造 $\mathfrak{A}$ は，領域 $A = |\mathfrak{A}|$ と，L の各関数記号に対応する A 上の関数，L の各関係記号に対応する A 上の関係から成り立っている．いま，$\mathfrak{A}, \mathfrak{B}$ をそれぞれ言語 L, L' における構造とし，$L \subset L'$ とする．このとき，$\mathfrak{B}$ が $\mathfrak{A}$ の拡張 (**expansion**), または $\mathfrak{A}$ が $\mathfrak{B}$ の縮約 (**reduct**) であるというのは，$|\mathfrak{A}| = |\mathfrak{B}|$ で，L の各記号に対応する $\mathfrak{A}, \mathfrak{B}$ の解釈が一致する場合である．

たとえば，算術の標準モデル $\mathfrak{N} = (\mathbf{N}, +, \cdot, \mathrm{S}, 0)$ から掛け算 $\cdot$ を除いた構造 $\mathfrak{N}' = (\mathbf{N}, +, \mathrm{S}, 0)$ は $\mathfrak{N}$ の縮約である．構造におけるこのような簡単な変更が，モデル全体として大きな変化をもたらすことがある．$Th(\mathfrak{N}_\mathbf{N})$ が算術的に定義できない集合であることは前に述べたが，$Th(\mathfrak{N}'_\mathbf{N})$ は再帰的な集合であり (プレスバーガー (M. Presburger) の定理)，公理化可能でもある．

今度は，$L \subset L'$ となる言語 L, L' における理論を適当に選んで T, T' とする．このとき，小さい方の言語 L の任意の文 σ に対して，

$$T \vdash \sigma \Leftrightarrow T' \vdash \sigma$$

が成り立つならば，T' は T の**保存的拡大** (**conservative extension**) であるという．以下，保存的拡大に関する二，三の定理を，構造の拡張という観点から見て証明しよう．

定理 3.9　$T \vdash \exists x \varphi(x)$ ならば，新しい定数 c を用いて拡大した理論 $T' = T \cup \{\varphi(c)\}$ は T の保存的拡大である．

[証明]　明らかに，T の定理は T' の定理である．あとは，c を含まない文で T' の定理となるもの σ を任意に選んで，$T \vdash \sigma$ を示せばよい．$\mathfrak{A}$ を T の任意のモデルとする．(モデルがなければ，T は矛盾しており何も証明する必要がない．) $T \vdash \exists x\, \varphi(x)$ だから，$\mathfrak{A}$ において $\varphi(a)$ を成り立たせる要素 $a \in |\mathfrak{A}|$ が存在する．いま，新しい定数 c の解釈を $c^{\mathfrak{A}} = a$ として，それを $\mathfrak{A}$ に加えた構造 $\mathfrak{A}^* = \mathfrak{A} \cup \{c^{\mathfrak{A}}\}$ を考えれば，明らかに $\mathfrak{A}^* \vdash T \cup \{\varphi(c)\}$. つまり，$\mathfrak{A}^*$ は T' のモデルである．すると，σ は T' の定理だから，$\mathfrak{A}^*$ で真となる．また，σ は c を含まない文だから，$\mathfrak{A}^*$ における c の解釈は σ の真偽と無関係であり，それを取り除いた $\mathfrak{A}$ でも σ は真となるはずである．最後に，$\mathfrak{A}$ は T の任意のモデルだから，完全性定理により $T \vdash \sigma$ がいえる．□

問題．上の定理を，完全性定理を用いずに証明せよ．ヒント：$T \cup \{\varphi(c)\} \vdash \sigma$ ならば，$T \vdash \varphi(c) \to \sigma$. これから，$T \vdash \exists x\, \varphi(x) \to \sigma$ を導く．

定理 3.10　$\varphi(x_0, \cdots, x_{n-1}, y)$ を言語 L における論理式で，$x_0, \cdots, x_{n-1}, y$ 以外の自由変数を持たないものとする．このとき，$T \vdash \forall x_0 \cdots \forall x_{n-1}\, \exists y\, \varphi(x_0, \cdots, x_{n-1}, y)$ ならば，新しい n 変数関数記号 f を用いた拡大理論 $T' = T \cup \{\forall x_0 \cdots \forall x_{n-1}\, \varphi(x_0, \cdots, x_{n-1}, f(x_0, \cdots, x_{n-1}))\}$ は T の保存的拡大である．

[証明]　定理 3.9 の定数による拡大とほぼ同様に証明できる．$T \vdash \forall x_0 \cdots \forall x_{n-1}\, \exists y$

$\varphi(x_0, \cdots, x_{n-1}, y)$ ならば，T の任意のモデル $\mathfrak{A}$ において，$\forall x_0 \cdots \forall x_{n-1}\, \varphi(x_0, \cdots, x_{n-1}, f(x_0, \cdots, x_{n-1}))$ を成り立たせる関数 $f^{\mathfrak{A}}$ が作れること (選択公理を使用) に注意．□

次の系は上の定理からただちに導かれるが，その主張を見やすくするために，ここで 2 つの論理記号を導入しておく．まず，$\phi \leftrightarrow \psi$ は $(\phi \to \psi) \wedge (\psi \to \phi)$ の略記と定義する．また，$\exists! y\, \psi(y)$ は $\exists y\, \psi(y) \wedge \forall y_1 \forall y_2 (\psi(y_1) \wedge \psi(y_2) \to y_1 = y_2)$ の略記であり,「$\psi(y)$ を満たす y がただ一つ存在する」ことを意味する．

系 3.11 $\varphi(x_0, \cdots, x_{n-1}, y)$ は，$x_0, \cdots, x_{n-1}, y$ 以外の自由変数を持たないものとする．このとき，$T \vdash \forall x_0 \cdots \forall x_{n-1}\, \exists! y\, \varphi(x_0, \cdots, x_{n-1}, y)$ ならば，新しい関数記号 f を用いて拡大した理論 $T' = T \cup \{\forall x_0 \cdots \forall x_{n-1} \forall y (\varphi(x_0, \cdots, x_{n-1}, y) \leftrightarrow f(x_0, \cdots, x_{n-1}) = y)\}$ は T の保存的拡大である．

上の系の前提のもとで，関数記号 f を含む論理式 ψ が与えられたとき，次のような変形を行って，f を含まない論理 ψ^{-f} を作る：

(1) ψ に含まれる項 $f(t_0, \cdots, t_{n-1})$ で，どの引数 t_i にも f を含まないものを選ぶ．

(2) ψ において，(1) で選んだ項 (の一つの出現) を新しい変数 y に置き換えてできる論理式を $\psi_1(y)$ とする．

(3) $\psi' = \exists y (\varphi(t_0, \cdots, t_{n-1}, y) \wedge \psi_1(y))$ とおく．

(4) ψ' がさらに f を含むときは，$\psi = \psi'$ として，(1) へ．そうでなければ，ψ' が求める ψ^{-f} である．

こうして，作った ψ^{-f} について，

$$T' \vdash \psi \leftrightarrow \psi^{-f}$$

となることは容易にわかる．したがって，T' における関数記号 f を用いた議論展開は，f を含まない議論に翻訳でき，T' の保存的拡大性からそれは T における議論ともみなせる．このことから，$T \vdash \forall x_0 \cdots \forall x_{n-1}\, \exists! y\, \varphi(x_0, \cdots, x_{n-1}, y)$ な

らば，$\varphi(x_0, \cdots, x_{n-1}, f(x))$ を満たす f が最初から T に入っていると考えても，T の証明可能性や表現可能性は変わらない．

関係についても次のことがいえる．

定理 3.12　$\varphi(x_0, \cdots, x_{n-1})$ は，$x_0, \cdots, x_{n-1}$ 以外の自由変数を持たないものとする．新しい関係記号 R をつかって，$T' = T \cup \{\forall x_0 \cdots \forall x_{n-1}(\varphi(x_0, \cdots, x_{n-1}) \leftrightarrow R(x_0, \cdots, x_{n-1}))\}$ とすると，T' は T の保存的拡大である．

論理式 ψ に含まれるすべての $R(t_0, \cdots, t_{n-1})$ を $\varphi(t_0, \cdots, t_{n-1})$ に置き換えた式を ψ^{-R} とすれば，やはり

$$T' \vdash \psi \leftrightarrow \psi^{-R}$$

がいえる．したがって，このような関係記号 R も最初から T に入っていると考えてよい．

最後に，1 階述語論理の自然な拡張である**多領域論理** (**many sorted logic**) について述べる．数学の理論では，2 種類以上の異なった対象を同時に扱うことがよくある．たとえば，ベクトル空間ならスカラーとベクトル，ユークリッド幾何なら点と線と面，などである．このような場合，複数の構造 $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \cdots$ の個別の性質と，それらの構造にまたがる性質を同時に議論する必要がある．

この状況は一見複雑に見えるが，容易に普通の 1 階述語論理の枠組みに納めることができる．すなわち，全体領域として $U = A \cup B \cup C \cup \cdots$ を取り，各領域 $A, B, C, \cdots$ をそれぞれ 1 変数述語で表現すればよい．ユークリッド幾何を普通の 1 階述語論理で議論するなら，“x は点である”，“x は線である”，“x は面である” という意味の関係記号をそれぞれ $P(x), L(x), F(x)$ とし，たとえば，“すべての点 x について，$\cdots$” は $\forall x(P(x) \rightarrow \cdots)$ で表せばよい．しかし，表記の簡便さのために，異なる種類の対象には，異なる変数記号を用い，それらは対応する領域だけを動くものと約束することが多い．ユークリッド幾何の場合，点の変数は小文字，線は大文字，面はギリシャ文字などとする．また，自然数と自然数の集合という 2 種類の対象をもっている 2 階算術の体系では，自然数の変数には小文字，

集合の変数には大文字を使うことでそれぞれの変域を区別する.

第 4 講　再帰的関数

4.1　原始再帰的関数

「関数」を英語では function (機能，機構の意) というが，その機構が機械仕掛けになりうるもの，要するに計算機を使ってインプットとアウトプットの関係として実現できる関数が計算可能な関数である．本講では，主として，自然数 (の組) から自然数への関数，いわゆる数論的関数について，計算可能な関数のクラスを考えて行こう．

本節では，計算可能な関数の一種である原始再帰的関数について述べる．歴史的には，現在の原始再帰的を「再帰的」，そして再帰的を「一般再帰的」と呼ぶことがあったが，以下の定義を見ていただければそれが納得できよう．原始再帰的関数およびそれを特性関数とするような原始再帰的関係は，形式体系についての議論 (メタ数学) を形式化する際に重要な役割を担う．実際，これらの概念は不完全性定理の証明の中で生まれたものだった．

定義．原始再帰的関数 (**primitive recursive function**) は以下のように定義される：

(1)　**ゼロ関数** $\mathrm{Z}() = 0$, **後者関数** $\mathrm{S}(x) = x+1$, **射影関数** $\mathrm{P}^n_i(x_1, x_2, \cdots, x_n) = x_i (1 \leqq i \leqq n)$ は原始再帰的関数である．(注：ゼロ関数は，0 変数の関数，つまり定数 0 である．)

(2a) **関数合成**．$g_i : \mathbf{N}^n \to \mathbf{N}$, $h : \mathbf{N}^m \to \mathbf{N}$ $(1 \leqq i \leqq m)$ が原始再帰的関数のとき，

$$f(x_1, \cdots, x_n) = h(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$$

で定義される合成関数 $f = h(g_1, \cdots, g_m) : \mathbf{N}^n \to \mathbf{N}$ は原始再帰的関数である．

(2b) **原始再帰法**．$g : \mathbf{N}^n \to \mathbf{N}, h : \mathbf{N}^{n+2} \to \mathbf{N}$ が原始再帰的関数のとき，

$$f(x_1, \cdots, x_n, 0) = g(x_1, \cdots, x_n)$$

$$f(x_1, \cdots, x_n, y+1) = h(x_1, \cdots, x_n, y, f(x_1, \cdots, x_n, y))$$

で定義される関数 $f : \mathbf{N}^{n+1} \to \mathbf{N}$ は原始再帰的関数である．

上の (2b) において，g と h が計算可能な全域関数 (自然数全体で定義される関数) であれば，それから定義される関数 f も計算可能な全域関数であることは容易にわかる．したがって，任意の原始再帰的関数が計算可能な全域関数であることは明らかである．(基礎論以外で) ふだん扱っている算術的関数のほとんどは原始再帰的である．原始再帰的関数の例をあげる前に，次の性質に注意しておこう．

補題 4.1 $f(x_1, \cdots, x_n)$ を原始再帰的 n 変数関数とする．いま，m 個の変数のリスト $y_1, \cdots, y_m$ から n 個の変数 $y_{i_1}, \cdots, y_{i_n}$ (重複を許す) を適当な順で選び，

$$f'(y_1, \cdots, y_m) = f(y_{i_1}, \cdots, y_{i_n})$$

によって，m 変数関数 f' を定義すると，f' も原始再帰的になる．

[証明] まず，f が定数の場合を考える．このときは，m 変数の定数関数 f' が原始再帰的であることを m に関する数学的帰納法で証明する．$m = 0$ ならば，$f'() = f()$ だから明らか．次に，m 変数関数 $f_m(y_1, \cdots, y_m) = f()$ が原始再帰的であると仮定する．すると，$(m+1)$ 変数関数 $f_{m+1}(y_1, \cdots, y_m, y_{m+1}) = f()$ は以下のように定義できる：

$$f_{m+1}(y_1, \cdots, y_m, 0) = f_m(y_1, \cdots, y_m)$$

$$f_{m+1}(y_1, \cdots, y_m, z+1) = \mathrm{P}^{m+2}_{m+2}(y_1, \cdots, y_m, z, f_{m+1}(y_1, \cdots, y_m, z)).$$

したがって，$f_{m+1}(y_1, \cdots, y_m, y_{m+1})$ も原始再帰的である．

f の元数 $n > 0$ のとき．f' は，以下のように定義できる：

$$f'(y_1, \cdots, y_m) = f(\mathrm{P}^m_{i_1}(y_1, \cdots, y_m), \cdots, \mathrm{P}^m_{i_n}(y_1, \cdots, y_m)).$$

よって，f' は原始再帰的である．□

それでは，原始再帰的関数の例を見ていこう．

例 1． 1 変数の定数関数 $f(x) = n$ は原始再帰的である．たとえば，$n = 3$ のと

き，$f(x) = \mathrm{S}(\mathrm{S}(\mathrm{S}(\mathrm{Z}())))$ である．(厳密には上の補題が使われることに注意！)

例 2．前者関数 $\mathrm{M}(x) = x - 1$ (ただし，$x = 0$ のときは $\mathrm{M}(x) = 0$ とする) は原始再帰的である．実際，原始再帰法により，

$$\mathrm{M}(0) = 0 = \mathrm{Z}()$$

$$\mathrm{M}(x+1) = x = \mathrm{P}^2_1(x, \mathrm{M}(x)).$$

例 3．たし算 $\mathrm{plus}(x, y)$ は

$$\mathrm{plus}(x, 0) = x$$

$$\mathrm{plus}(x, y+1) = \mathrm{S}(\mathrm{plus}(x, y))$$

で定義される．掛け算 $\mathrm{times}(x, y)$ は $\mathrm{plus}(x, y)$ を使って，

$$\mathrm{times}(x, 0) = 0$$

$$\mathrm{times}(x, y+1) = \mathrm{plus}(x, \mathrm{times}(x, y))$$

とすればよい．

慣習に従い，$\mathrm{plus}(x, y)$ を $x + y$, $\mathrm{times}(x, y)$ を $x \cdot y$ と書き，今後は関数の定義も直接そのような書き方で行う．たとえば，引き算 $x \dot{-} y$ の定義を以下のように書く：

$$x \dot{-} 0 = x$$

$$x \dot{-} (y+1) = \mathrm{M}(x \dot{-} y).$$

問題 1．x^y, $x!$, $\max\{x, y\}$ が原始再帰的関数であることを示せ．

問題 2．$f(x_1, \cdots, x_n, y)$ が原始再帰的ならば，$F(x_1, \cdots, x_n, z) = \Sigma_{y<z} f(x_1, \cdots, x_n, y)$ と $G(x_1, \cdots, x_n, z) = \Pi_{y<z} f(x_1, \cdots, x_n, y)$ も原始再帰的になることを示せ．

4.2　原始再帰的集合

定義．n 項関係 $R \subset \mathbf{N}^n$ が原始再帰的であるとは，

$$\chi_R(x_1, \cdots, x_n) = \begin{cases} 1, & R(x_1, \cdots, x_n) \text{ のとき} \\ 0, & \text{そうでないとき} \end{cases}$$

となる特性関数 $\chi_R : \mathbf{N}^n \to \{0, 1\}$ が原始再帰的になることである．

例 4．$x < y$ は原始再帰的である．実際，

$$\chi_<(x, y) = (y \dot{-} x) \dot{-} \mathrm{M}(y \dot{-} x)$$

である．(確かめよ)

補題 4.2　原始再帰的な n 項関係 A, B に対し，

$$\neg A, A \wedge B, A \vee B$$

も原始再帰的である．

[証明]　$\chi_{\neg A} = 1 \dot{-} \chi_A$. $\chi_{A \wedge B} = \chi_A \cdot \chi_B$. $\chi_{A \vee B} = 1 \dot{-} \{(1 \dot{-} \chi_A) \cdot (1 \dot{-} \chi_B)\}$. □

補題 4.3　2 つの原始再帰的 n 変数関数 g, h と，原始再帰的 n 項関係 R が与えられたとき，

$$f(x_1, \cdots, x_n) = \begin{cases} g(x_1, \cdots, x_n), & R(x_1, \cdots, x_n) \text{ のとき} \\ h(x_1, \cdots, x_n), & \text{そうでないとき} \end{cases}$$

で定義される関数 f は原始再帰的である．

[証明]　$f = g \cdot \chi_R + h \cdot \chi_{\neg R}$. □

例 5．$x = y$ は原始再帰的である．なぜなら，$x = y \Leftrightarrow \neg(x < y) \wedge \neg(y < x)$.

　これを使えば，次は容易に示せる．

補題 4.4　原始再帰的関数のグラフは原始再帰的である．

問題 3. $A(x_1, \cdots, x_n, y)$ が原始再帰的ならば, $\forall y < zA(x_1, \cdots, x_n, y)$ および $\exists y < zA(x_1, \cdots, x_n, y)$ も原始再帰的である．ヒント：問題 2 を使う．

例 6. $\mathrm{prime}(x) =$ "x は素数である" は原始再帰的関係である．実際,

$$\mathrm{prime}(x) \Leftrightarrow x > 1 \wedge \neg\exists y < x\ \exists z < x(y \cdot z = x).$$

補題 4.5　$A(x_1, \cdots, x_n, y)$ が原始再帰的ならば,

$$\mu y < zA(x_1, \cdots, x_n, y) = \min(\{y < z : A(x_1, \cdots, x_n, y)\} \cup \{z\})$$

で定義される関数 $\mu y < zA$ は原始再帰的関数である．

[証明]　$\mu y < zA = \Sigma_{w<z}\Pi_{y \leq w}\chi_{\neg A}$. □

例 7. $x \div y = \mu z < x(x < y \cdot (z+1))$ は原始再帰的である．

例 8. $\mathrm{p}(x) =$ "x 番目の素数" とする．すなわち, $\mathrm{p}(0) = 2, \mathrm{p}(1) = 3, \mathrm{p}(2) = 5, \cdots$. このとき, $\mathrm{p}(x)$ は次のように定義される原始再帰的関数である：

$$\mathrm{p}(x+1) = \mu y < \mathrm{p}(x)! + 2\ (\mathrm{p}(x) < y \wedge \mathrm{prime}(y)).$$

例 9. 自然数の有限列 $(x_0, \cdots, x_{n-1})$ を 1 つの自然数 $x = \mathrm{p}(0)^{x_0+1} \cdot \mathrm{p}(1)^{x_1+1} \cdot \cdots \cdot \mathrm{p}(n-1)^{x_{n-1}+1}$ でコード化する．n を固定すれば，この対応は $\mathbf{N}^n$ から $\mathbf{N}$ への原始再帰的関数である．逆に，コード x が与えられたとき，それが指し示す列の i 番目の要素 x_i を取り出す関数 $\mathrm{c}(x, i)$ は,

$$x_i = \mathrm{c}(x, i) = \mu y < x\ (\neg\exists z < x\ \ \mathrm{p}(i)^{y+2} \cdot z = x)$$

で与えられる．また，コード x の列の長さ $\mathrm{leng}(x)$ は

$$\mathrm{leng}(x) = \mu i < x\ (\neg\exists z < x\ \ \mathrm{p}(i) \cdot z = x)$$

で定義する．これらの関数は，どの列のコードにもならない自然数 x についても何らかの値をとる全域的な関数である．さらに，自然数 x が列のコードになる条件 $\mathrm{Seq}(x)$ は

$$\mathrm{Seq}(x) \Leftrightarrow \forall i < x \forall z < x\ (\mathrm{p}(i) \cdot z = x \rightarrow i \leq \mathrm{leng}(x))$$

と表せる．

4.3 再帰的関数

ここで扱う再帰的関数は，原始再帰的関数より一般的な計算可能関数である．

定義． **再帰的関数 (recursive function)** を以下のように定義する：

(1) **ゼロ関数** Z, **後者関数** S, **射影関数** P_i^n は再帰的関数である．

(2a) **関数合成**．再帰的関数を合成してつくられる関数は再帰的関数である．

(2b) **原始再帰法**．再帰的関数から再帰的に定義される関数は再帰的関数である．

(2c) **最小化**．$g : \mathbf{N}^{n+1} \to \mathbf{N}$ は再帰的関数で，$\forall x_1 \cdots \forall x_n \, \exists y \; g(x_1, \cdots, x_n, y) = 0$ を満たすとする．このとき，$g(x_1, \cdots, x_n, y) = 0$ となる最小の y を $\mu y(g(x_1, \cdots, x_n, y) = 0)$ で表し，

$$f(x_1, \cdots, x_n) = \mu y(g(x_1, \cdots, x_n, y) = 0)$$

で定義される関数 $f : \mathbf{N}^n \to \mathbf{N}$ は再帰的関数である．

再帰的関数は，原始再帰的関数と同様，計算可能な全域関数である．原始再帰的関数との定義の違いは上の (2c) だけだが，全域性を保つための条件 $\forall x_1 \cdots \forall x_n \exists y \; g(x_1, \cdots, x_n, y) = 0$ が形式上厄介な問題を生じる．この条件式がどの立場で証明できるかによって，再帰的関数のクラスが変わってくるからである．たとえば，ペアノ算術で認めれる再帰的関数のクラスと，ZF 集合論で認められる再帰的関数のクラスは一致していない．これがパート C における独立性証明のカギになる．

さて，それならば，(2c) において問題の条件を取り除くとどうなるだろうか？そのようにして定義される関数を再帰的部分関数という．正確な定義を述べるために，2 つの部分関数 $f(x_1, \cdots, x_n)$, $g(x_1, \cdots, x_n)$ の間の等号 $\sim$ を次のように定める．f と g が同じ定義域をもち，その上で両関数の値が一致するとき，$f \sim g$ とする．定数 c に対しては，$f(x_1, \cdots, x_n) \sim c$ は $f(x_1, \cdots, x_n) = c$ と同じ意味である．

定義. 再帰的部分関数を以下のように定義する：

(1)　ゼロ関数 Z, 後者関数 S, 射影関数 P_i^n は再帰的部分関数である．

(2a) **関数合成．** $g_i : \mathbf{N}^n \to \mathbf{N}, h : \mathbf{N}^m \to \mathbf{N} (1 \leqq i \leqq m)$ が再帰的部分関数のとき，

$$f(x_1, \cdots, x_n) \sim h(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$$

で定義される合成関数 $f = h(g_1, \cdots, g_m) : \mathbf{N}^n \to \mathbf{N}$ は再帰的部分関数である．ただし，$h(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$ は，各 $g_i(x_1, \cdots, x_n) = y_i$ が定義され，$h(y_1, \cdots, y_m) = z$ が定義されるときに限り定義されて，値 z をとる．

(2b) **原始再帰法．** $g : \mathbf{N}^n \to \mathbf{N}, h : \mathbf{N}^{n+2} \to \mathbf{N}$ が再帰的部分関数のとき，

$$f(x_1, \cdots, x_n, 0) \sim g(x_1, \cdots, x_n)$$

$$f(x_1, \cdots, x_n, y+1) \sim h(x_1, \cdots, x_n, y, f(x_1, \cdots, x_n, y))$$

で定義される関数 $f : \mathbf{N}^{n+1} \to \mathbf{N}$ は再帰的部分関数である．

(2c) **最小化．** $g : \mathbf{N}^{n+1} \to \mathbf{N}$ を再帰的部分関数とする．「$g(x_1, \cdots, x_n, c) = 0$ で，かつ各 $z < c$ に対し $g(x_1, \cdots, x_n, z)$ が定義され 0 以外の値をとる」ならば $\mu y(g(x_1, \cdots, x_n, y) = 0) = c$ とし，そのような c が存在しないとき $\mu y(g(x_1, \cdots, x_n, y) = 0)$ は定義されないとする．このとき，

$$f(x_1, \cdots, x_n) \sim \mu y(g(x_1, \cdots, x_n, y) = 0)$$

となる関数 $f : \mathbf{N}^n \to \mathbf{N}$ は再帰的部分関数である．

再帰的関数が再帰的部分関数であることはただちに言えるが，全域的な再帰的部分関数が再帰的関数になることは明らかではない．(上の (2c) で，g が全域的出なくても，f が全域的になる場合があることに注意．) しかし，次に述べる再帰的部分関数の標準形定理からこのことは簡単に導ける．

定理 4.6 (クリーネ (S. Kleene) の標準形定理) 原始再帰的関数 $U(y)$ と原始再帰的関係 $T_n(e, x_1, \cdots, x_n, y)$ が存在して，任意の n 変数再帰的部分関数

$f(x_1,\cdots,x_n)$ は，ある e について，

$$f(x_1,\cdots,x_n) \sim U(\mu y T_n(e,x_1,\cdots,x_n,y))$$

と表せる．ここで，$\mu y T_n(e,x_1,\cdots,x_n,y)$ は $\mu y((1-\chi_{T_n}(e,x_1,\cdots,x_n,y))=0)$ のことである．

[証明のアイデア]　何らかの計算モデルを介在させない限り，定理を満たす U と T_n を構成するのは困難である．ここでは，**(決定性) チューリング (A. Turing) 機械**を使って考えよう．チューリング機械は，無限に延長可能な入出力兼作業用のテープをもっており，動作開始時にテープに書かれていた記号列 (数) に，停止時にテープに残る記号列 (数) を対応させることで，計算可能な関数を実現する．まず，任意の再帰的部分関数がチューリング機械によって表現できることは簡単にわかる．これは，再帰的部分関数の構成に関する帰納法で証明すればよい．あとは，チューリング機械によって計算できる関数が，$U(\mu y T_n(e,x_1,\cdots,x_n,y))$ の形で表せることを示せばよい．

チューリング機械の内部機構は有限的なものだから，各チューリング機械を自然数でコード化することが可能である．このコードは単なる製品番号である以上に，チューリング機械の設計図になっていると考えることもできる．いま，コード e をもつチューリング機械に入力列 $(x_1,\cdots,x_n)$ を与えて，それが停止するまでの計算状況 (内部状態とテープの状態) の遷移過程を逐一記録したものを y とする．計算が永久に停止しないこともあるので y が存在するとは限らないが，存在すれば有限列であるから自然数 $y=(y_0,\cdots,y_k)$ でコードできる．さて，コード e, 列 $(x_1,\cdots,x_n)$, およびコード y を与えて，y がコード e のチューリング機械に列 $(x_1,\cdots,x_n)$ を入力したときの計算過程の正しいコードになっているかどうかを検査する．これは，$y=(y_0,\cdots,y_k)$ において，各計算状況 y_i から次の計算状況 y_{i+1} への遷移が正しいかどうかチェックをすればよく，容易に原始再帰的関係として実現できる．すなわち，次を満たす原始再帰的関係 $T_n(e,x_1,\cdots,x_n,y)$ が存在する：

$T_n(e,x_1,\cdots,x_n,y) \Leftrightarrow y$ はコード e のチューリング機械に列 $(x_1,\cdots,x_n)$ を
入力したときの計算過程のコードである．

さらに，y が計算の全過程をコードしていれば，その最終状況におけるテープの状態，つまり出力の情報も y は含んでいる．それを取り出す原始再帰的関数を $U(y)$ とすれば，$U(\mu y T_n(e, x_1, \cdots, x_n, y))$ は，コード e をもつチューリング機械に列 $(x_1, \cdots, x_n)$ を入力したときの出力結果に他ならない．□

上の証明で構成した U と T_n を固定して，$U(\mu y T_n(e, x_1, \cdots, x_n, y))$ を指標 e の n 変数再帰的部分関数と呼び，$\{e\}^n(x_1, \cdots, x_n)$ あるいは簡単に $\{e\}(x_1, \cdots, x_n)$ と書く．このとき，標準形定理を次のように述べることがある．

標準形定理 (別形)　部分関数 f が再帰的であることと，f が指標をもつことは同値である．

また，$\{e\}$ の定義からただちに次のことがいえる．

定理 4.7 (枚挙定理)　$\{e\}(x_1, \cdots, x_n)$ は $e, x_1, \cdots, x_n$ に関する $(n+1)$ 変数の再帰的部分関数である．

定理 4.8 (パラメタ定理, S-m-n 定理)　原始再帰的関数 S^m_n が存在し，

$$\{e\}^{m+n}(x_1, \cdots, x_n, y_1, \cdots, y_m) \sim \{S^m_n(e, y_1, \cdots, y_m)\}^n(x_1, \cdots, x_n).$$

[証明のアイデア]　チューリング機械の設計図 e と列 $(y_1, \cdots, y_m)$ が予め与えられているとし，次のようなチューリング機械を作る．それは列 $(x_1, \cdots, x_n)$ を入力すると，その後ろに $(y_1, \cdots, y_m)$ を書き込んで $(x_1, \cdots, x_n, y_1, \cdots, y_m)$ としてから，コード e のチューリング機械の動作を模倣する．このチューリング機械の設計図は，e と $(y_1, \cdots, y_m)$ から簡単に，正確には原始再帰的に作成できる．すなわち，原始再帰的関数 S^m_n が存在して，$S^m_n(e, y_1, \cdots, y_m)$ がその設計図となる．□

定理 4.9 (再帰定理) $f(x_1, \cdots, x_n, y)$ を再帰的部分関数とする．このとき，e が存在して，

$$\{e\}^n(x_1, \cdots, x_n) \sim f(x_1, \cdots, x_n, e)$$

となる．

[証明] パラメタ定理により，$\{g(y)\}(x_1, \cdots, x_n) \sim \{y\}(x_1, \cdots, x_n, y)$ となる原始再帰的関数 $g(y)$ が存在する．すると，$f(x_1, \cdots, x_n, g(y))$ は再帰的部分関数であり，指標 d をもつ．そこで，$e = g(d)$ とおけばよい．実際，

$$\{g(d)\}(x_1, \cdots, x_n) \sim \{d\}(x_1, \cdots, x_n, d) \sim f(x_1, \cdots, x_n, g(d)). \quad \square$$

再帰定理を使うと，たとえば

$$\{e\}(x) \sim \{e\}(x-1) + \{e\}(x+1)$$

を満たす再帰的部分関数 $\{e\}$ が存在する．原始再帰法では，$\{e\}(x)$ の定義の右辺に $\{e\}(x+1)$ が現れることはなかった．しかし，この定理によれば，$\{e\}(x)$ を定義するのに $\{e\}$ のあらゆる情報を使うことができる．但し，注意すべきことは，この例でもそうだが，定義域が空になる関数も解になりうることである．もう少し実際的な応用例を見てみよう．

例 10． 値域が無限集合になる再帰的関数 f を任意に選ぶ．このとき，集合 $\{x : \forall y < x f(x) \neq f(y)\}$ も無限集合である．いま，この集合の要素を小さい方から並べ上げる再帰的関数 g がほしいとしよう．そこで，原始再帰法を使って，次のように定義したらどうだろうか：

$$g(0) = 0,$$

$$g(x) = \mu w \forall y \leq g(x \dot{-} 1) f(w) \neq f(y).$$

この定義では原始再帰法と最小化が同時に使われており，このままではわれわれの再帰的部分関数の定義に適合しない．しかし，再帰定理を用いれば，

$$g(x) \sim \begin{cases} 0 & x = 0 \text{ のとき} \\ \mu w \forall y \leq g(x \dot{-} 1) f(w) \neq f(y) & \text{そうでないとき} \end{cases}$$

のように，原始再帰法なしで再帰的部分関数 g ができる．この g が全域的になることは帰納法で簡単に証明できるから，g が求める再帰的関数である．

問題 4．次の等式で定義される関数 f (アッケルマン (**W. Ackermann**) 関数と呼ばれる) が再帰的関数であることを示せ：

$$f(0,y) = y+1$$

$$f(x+1,0) = f(x,1)$$

$$f(x+1,y+1) = f(x, f(x+1,y)).$$

さらに，この関数が次のような性質をもつことを示せ (やや難)．任意の原始再帰的関数 $g(x,y)$ に対して，ある c が存在し，

$$g(x,y) < f(c, \max\{x,y\}).$$

このことから，f 自身は原始再帰的関数でないことがわかる．

4.4　再帰的関係と RE 集合

定義．n 項関係 $R \subset \mathbf{N}^n$ が再帰的 (**recursive**) であるとは，

$$\chi_R(x_1,\cdots,x_n) = \begin{cases} 1, & R(x_1,\cdots,x_n) \text{ のとき} \\ 0, & \text{そうでないとき} \end{cases}$$

となる特性関数 $\chi_R : \mathbf{N}^n \to \{0,1\}$ が再帰的になることである．

もちろん原始再帰的関係は再帰的である．次の 3 つの補題は，原始再帰的関係の場合と同様に証明できる．

補題 4.10　再帰的な n 項関係 A, B に対し，

$$\neg A, A \wedge B, A \vee B, \forall y < zA, \exists y < zA$$

も再帰的である．

補題 4.11　2 つの再帰的 n 変数関数 g, h と，再帰的 n 項関係 R が与えられた

とき,

$$f(x_1, \cdots, x_n) = \begin{cases} g(x_1, \cdots, x_n), & R(x_1, \cdots, x_n) \text{ のとき} \\ h(x_1, \cdots, x_n), & \text{そうでないとき} \end{cases}$$

で定義される関数 f は再帰的である.

補題 4.12 再帰的関数のグラフは再帰的である.

さらに,最後の補題の逆もいえる.

補題 4.13 再帰的グラフをもつ全域関数は再帰的関数である.

[証明] グラフ $F(x,y)$ をもつ関数は $\mu y F(x,y)$ (正確には $\mu y\ (1 - \chi_F(x,y) = 0)$) と表せるから,再帰的グラフをもつ関数は再帰的部分関数である.もし,それが全域的なら,クリーネの標準形定理より再帰的関数である.□

この補題の原始再帰的バージョンは成立しない.

問題 5 (やや難). 問題 4 で定義したアッケルマン関数のグラフは原始再帰的集合になることを示せ.

定義. n 項関係 $R \subset \mathbf{N}^n$ が再帰的に枚挙可能 (**recursively enumerable** 略して **RE**) であるとは,

$$f(x_1, \cdots, x_n) = \begin{cases} 1 & R(x_1, \cdots, x_n) \text{ のとき} \\ \text{未定義} & \text{そうでないとき} \end{cases}$$

となる部分関数 f が再帰的部分関数になることである.

ただちに分かることとして,どんな再帰的部分関数の定義域も RE である.また,どんな再帰的 (部分) 関数の値域も RE になることがいえ,「再帰的に枚挙可能」という名はじつはその性質を表している.他にも RE と同値な条件がたくさ

んあるが，基本的なものを次の補題にまとめておく．

補題 4.14　関係 $R \subset \mathbf{N}^n$ について，次の条件は同値である．

(1) R は再帰的に枚挙可能．

(2) R は空集合かある原始再帰的関数の値域になる．

(3) R は有限集合かある再帰的単射 (1 対 1 関数) の値域になる．

(4) R は空集合かある再帰的関数の値域になる．

(5) R はある再帰的部分関数の値域になる．

(6) ある原始再帰的関係 S が存在して，$R(x_1, \cdots, x_n) \Leftrightarrow \exists y\, S(x_1, \cdots, x_n, y)$.

(7) ある再帰的関係 S が存在して，$R(x_1, \cdots, x_n) \Leftrightarrow \exists y\, S(x_1, \cdots, x_n, y)$.

[証明]　まず，(1) ⇒ (6) ⇒ (7) ⇒ (1) を示そう．

(1) ⇒ (6) について．再帰的部分関数 f が

$$f(x_1, \cdots, x_n) = \begin{cases} 1, & R(x_1, \cdots, x_n) \text{ のとき} \\ \text{未定義}, & \text{そうでないとき} \end{cases}$$

を満たすとする．クリーネの標準形定理より，原始再帰的な U と T が存在して，

$$f(x_1, \cdots, x_n) \sim U(\mu y T(x_1, \cdots, x_n, y))$$

と書ける．したがって，$R(x_1, \cdots, x_n) \Leftrightarrow \exists y T(x_1, \cdots, x_n, y)$.

(6) ⇒ (7) は明らか．

(7) ⇒ (1). ある再帰的関係 S が存在し，$R(x_1, \cdots, x_n) \Leftrightarrow \exists y S(x_1, \cdots, x_n, y)$ とする．いま，$U(y) = 1$ となる原始再帰的関数 U を使って，$f(x_1, \cdots, x_n) \sim U(\mu y S(x_1, \cdots, x_n, y))$ と定義すれば，この f は (1) を満たす．

次に，(2) ⇒ (3) ⇒ (4) ⇒ (5) ⇒ (6) ⇒ (2) をいう．以下の議論を簡単にするため，$R \subset \mathbf{N}$ で，かつ (2)〜(5) の関数はすべて 1 変数であるとしよう．$\mathbf{N}^n$ と $\mathbf{N}$ の間には原始再帰的な 1 対 1 対応がある（4.2 節例 9 を参照）から，この仮定は結論を弱めない．

(2) ⇒ (3) について．R はある原始再帰的関数 f の値域で，かつ無限集合とする．再帰定理により，次を満たす再帰的関数 g が存在する (例 10) :

$$g(0) = 0,$$

$$g(x) = \mu w \forall y \leqq g(x \dot{-} 1) f(w) \neq f(y).$$

そして，$h(x) = f(g(x))$ とおけば，h は f と同じ値域をもつ再帰的単射となり，(3) が証明された．

(3) ⇒ (4) について．任意の有限集合が再帰的関数の値域になることに注意すればよい．

(4) ⇒ (5) は明らか．

(5) ⇒ (6). R は再帰的部分関数 $f(x)$ の値域であるとする．クリーネの標準形定理より，原始再帰的な U と T が存在して，

$$f(x) \sim U(\mu y T(x, y))$$

と書ける．すると，

$$\begin{aligned} R(z) &\Leftrightarrow z \in \mathrm{range}(f) \\ &\Leftrightarrow \exists x\, \exists y (T(x, y) \wedge U(y) = z) \\ &\Leftrightarrow \exists x (T(\mathrm{c}(x, 0), \mathrm{c}(x, 1)) \wedge U(\mathrm{c}(x, 1)) = z). \end{aligned}$$

ここで，$\mathrm{c}(x, i)$ は x でコードする列の i 番目の要素 x_i を取り出す原始再帰的関数 (例 9 参照)．最後の式のカッコの中は，原始再帰的関係になっているから，(6) がいえる．

(6) ⇒ (2) について．原始再帰的関係 S が存在し，$R(x) \Leftrightarrow \exists y\, S(x, y)$ とする．さらに，R は空集合でないとして，その 1 つの要素 d を選ぶ．そして，次のような原始再帰的関数 g を考える：

$$g(x) = \begin{cases} \mathrm{c}(x, 0), & S(\mathrm{c}(x, 0), \mathrm{c}(x, 1)) \text{ のとき} \\ d, & \text{そうでないとき} \end{cases}$$

このとき，$\mathrm{range}(g)$ が R に一致することは明らか．□

次の補題は簡単に証明できる．

補題 4.15　再帰的に枚挙可能な n 項関係 A, B に対し，

$$A \wedge B, A \vee B, \forall y < z\, A, \exists y < z\, A, \text{ そして } \exists y\, A$$

も再帰的に枚挙可能である．

補題 4.16　再帰的部分関数のグラフは再帰的に枚挙可能である．

[証明]　$f(x_1, \cdots, x_n)$ を再帰的部分関数とする．クリーネの標準形定理より，原始再帰的な U と T が存在して，

$$f(x_1, \cdots, x_n) \sim U(\mu y T(x_1, \cdots, x_n, y))$$

と書ける．したがって，

$$f(x_1, \cdots, x_n) = z \Leftrightarrow \exists y (T(x_1, \cdots, x_n, y) \wedge \forall w < y \, \neg T(x_1, \cdots, x_n, w) \\ \wedge U(y) = z).$$

右辺は原始再帰的関係の前に $\exists y$ が置かれたものだから，再帰的に枚挙可能になる．

□

補題 4.17　再帰的に枚挙可能なグラフをもつ関数は再帰的部分関数である．

[証明]　再帰的枚挙可能なグラフ $F(x, y)$ をもつ関数は $\mu y F(x, y)$ と表せるから再帰的部分関数になるという推論は間違いである．$\mu y F(x, y)$ が定義されるためには，各 $z < y$ について $F(x, z)$ が定義されている必要があるが，ここではその保証が何もないからである．そこで，まず原始再帰的関係 S を用いて，$F(x, y) \Leftrightarrow \exists z \, S(x, y, z)$ と表す．そして，$\mu y S(x, \mathrm{c}(y, 0), \mathrm{c}(y, 1))$ を考えれば，$S(x, \mathrm{c}(y, 0), \mathrm{c}(y, 1))$ が全域的なのでこれは問題ない定義である．そして，求める関数は $\mathrm{c}(\mu y S(x, \mathrm{c}(y, 0), \mathrm{c}(y, 1)), 0)$ で与えられる．□

問題 6．RE 集合が無限集合であれば，再帰的な無限部分集合を含むことを示せ．ヒント：無限の RE 集合 R が再帰的関数 $f(x)$ の値域として与えられているとせよ．まず，与えられた n より大きな $f(x)$ の値を取り出す再帰的関数 $F(n) = \mathrm{c}(\mu y (n < f(\mathrm{c}(y, 0)) = \mathrm{c}(y, 1)), 1)$ を定義する．そして，$g(0) = f(0), g(x+1) = F(g(x))$ とおくと，$\{y : \exists x \leqq y f(x) = y\}$ が求める集合になる．

次の 2 つの定理は，再帰的集合と RE 集合の関係についての重要な結果である．

定理 4.18　n 項関係 R が再帰的集合であるための必要十分条件は，R とその否

定 $\neg R = \mathbf{N}^n - R$ がともに RE になることである．

[証明] 必要性は明らかである．十分であることを示すため，R と $\neg R$ がともに RE であるとする．補題 4.14 より，原始再帰的関係 S, T が存在して，$R(x_1, \cdots, x_n) \Leftrightarrow \exists y S(x_1, \cdots, x_n, y)$, $\neg R(x_1, \cdots, x_n) \Leftrightarrow \exists y T(x_1, \cdots, x_n, y)$ と表せる．$R \vee \neg R$ より，$\exists y(S \vee T)$ だから，$\mu y S \vee T$ は再帰的 n 変数関数になる．すると容易に，$R(x_1, \cdots, x_n) \Leftrightarrow S(x_1, \cdots, x_n, \mu y S \vee T)$ がいえるから，R は再帰的関係である．

□

定理 4.19 再帰的でない RE 集合が存在する．

[証明] $K = \{e : e \in \mathrm{dom}(\{e\})$ (すなわち $\{e\}(e)$ が値をもつ) $\}$ とおく．$\{x\}(y)$ は 2 変数の再帰的部分関数と考えられるから，K は RE 集合である．あとは，$\neg K$ が RE でないことをいえばよい．$\neg K$ が RE として，$\neg K = \mathrm{dom}(\{d\})$ とする．$d \in K \Leftrightarrow d \in \mathrm{dom}(\{d\}) \Leftrightarrow d \in \neg K$ だから，$d \in K$ でも $d \in \neg K$ でも矛盾が生じる．よって，$\neg K$ は RE ではなく，したがって K は再帰的でない．□

例 11． 次の集合も再帰的でない再帰的枚挙可能集合である：

$$K_0 = \{(x, e) : x \in \mathrm{dom}(\{e\})\},$$

$$K_1 = \{e : \mathrm{dom}(\{e\}) \neq \emptyset\}.$$

問題 7． 2 つの RE 集合 $A = \{e : \{e\}(e) \sim 0\}, B = \{e : \{e\}(e) \sim 1\}$ に対し，A を含み，B との共通部分が空になるような再帰的集合 C は存在しないことを示せ．(このとき，A と B とは**再帰的に分離不能 (recursively inseparable)** であるという．) ヒント： もし A と B を分離する再帰的集合 C があれば，その特性関数の指標を d として，上の定理と同様に矛盾を導け．

上の問題の結果は，パート D で用いられる．

4.5　β関数によるコード化

4.2 節の例 9 では自然数の有限列を素数の巾乗を用いて一つの自然数にコード化する方法を紹介した．しかし，形式的算術では指数関数が最初から与えられているわけではないので，それとは異なるコード化技法が必要になる．ここでは，中国剰余定理に基づいて定義されるゲーデルの β関数によるコード化を導入する．この方法は 4.6 節やパート B で用いられるが，その際ここでの議論の精密化が必要となるので，以下では各定理の証明をややていねいに与えることにする．

自然数 x が 自然数 y の約数であることを $x|y$ と記し，x を y で割った余りを $\mathrm{rm}(x,y)$ で表す．また，x, y が 2 以上の共約数を持たないとき，x と y は互いに素であるという．

補題 4.20　1 以上の自然数 m, n が互いに素ならば，$m{\cdot}x - n{\cdot}y = 1$ なる自然数 x, y が存在する．

[証明]　自然数 a について，条件

$$m{\cdot}x - n{\cdot}y = a \text{ なる自然数 } x,\ y \text{ が存在する}$$

が成り立つことを $\mathcal{P}(a)$ と記すことにする．すると次の (1)(2) は簡単に示される．

(1) $\mathcal{P}(m)$ および $\mathcal{P}(n)$.

(2) $\mathcal{P}(d)$ ならば $\mathcal{P}(q{\cdot}d)$. (d, q は任意の自然数)

さらに，次も成り立つ．

(3) ($a > b$, $\mathcal{P}(a)$, $\mathcal{P}(b)$) ならば $\mathcal{P}(a{-}b)$.

なぜなら，$m{\cdot}x - n{\cdot}y = a$ かつ $m{\cdot}u - n{\cdot}v = b$ ならば

$$m{\cdot}[x + n{\cdot}v + (n-1){\cdot}u] - n{\cdot}[y + m{\cdot}u + (m-1){\cdot}v] = a - b$$

だからである．さて，ここで d を $\mathcal{P}(d)$ が成り立つ 0 でない最小の自然数とする．すると次が成り立つ．

(4) $\mathcal{P}(a)$ ならば $d|a$. (a は任意の自然数)

なぜなら，$r = \mathrm{rm}(a,d)$ とすると適当な q に対して $r = a - q{\cdot}d$ であり，(2), (3) および d の最小性により，$r = 0$ になるからである．ところで m, n は互いに素

だったので，(1), (4) により $\mathcal{P}(1)$ となる．□

補題 4.21 自然数 s, t, m, n が $s < m$ かつ $t < n$ であって，m と n が互いに素ならば，

$$\mathrm{rm}(k, m) = s,\ \mathrm{rm}(k, n) = t$$

なる自然数 k が存在する．

[証明] $s = t$ の場合には $k = m{\cdot}n + s$ とすればよい．$s \neq t$ の場合には，一般性を失うことなく $s < t$ と仮定してよい．すると補題 4.20 とその証明中の (2) によって $\mathcal{P}(t-s)$ となり，

$$k = m{\cdot}x + s = n{\cdot}y + t$$

とできる．□

さて，$f(x) > 0$ なる全域関数 f に対して，

$$\bigvee_{i=k}^{n} f(i)$$

で $f(k), f(k+1), \cdots, f(n)$ の最小公倍数を表すものとする．

定理 4.22 (中国剰余定理)

n を任意の自然数とし，$f(x)$, $g(x)$ を以下を満たす全域関数とする．

- $0 \leqq i < j \leqq n$ ならば $g(i)$ と $g(j)$ は互いに素．
- $0 \leqq i \leqq n$ ならば $f(i) < g(i)$.

すると次の条件を満たす自然数 a が存在する．

- $a < \bigvee_{i=0}^{n} g(i)$.
- $0 \leqq i \leqq n$ ならば $\mathrm{rm}(a, g(i)) = f(i)$.

[証明] n に関する帰納法による．$n = 0$ のときには $a = f(0)$ とすればよい．$n = n' + 1$ のときには帰納法の仮定によって，

- $a' < \bigvee_{i=0}^{n'} g(i)$,

- $0 \leqq i \leqq n'$ ならば $\mathrm{rm}(a', g(i)) = f(i)$,

となるような自然数 a' が存在する．$\bigvee_{i=0}^{n'} g(i)$ と $g(n'+1)$ が互いに素であることは簡単に示されるので，補題 4.21 を

$$s = a', \quad t = f(n'+1), \quad m = \bigvee_{i=0}^{n'} g(i), \quad n = g(n'+1)$$

(この n は補題中の n)

として適用すると,

$$\mathrm{rm}(k, \bigvee_{i=0}^{n'} g(i)) = a', \quad \mathrm{rm}(k,\ g(n'+1)) = f(n'+1),$$

なる自然数 k が得られる．そしてこれを用いて

$$a = \mathrm{rm}(k, \bigvee_{i=0}^{n'+1} g(i))$$

とすれば，これが求める a になることが簡単に示される．□

補題 4.23　n, m を $1 \leqq n \leqq m$ なる自然数とし，$d = \bigvee_{x=1}^{m} x$ とする．すると，$0 \leqq i < j \leqq n$ なるどんな i, j に対しても，自然数

$$(i+1)\cdot d+1, \quad (j+1)\cdot d+1$$

は互いに素である．

[証明]　互いに素でないと仮定する．すなわち，$0 \leqq i < j \leqq n$ であって

(†) $p|((i+1)\cdot d+1)$　かつ　$p|((j+1)\cdot d+1)$,

となる i, j および素数 p が存在するとする．すると (†) より $p|((j-i)\cdot d)$ となるが，このことから $p \leqq m$ であることがわかる．(なぜなら，$j-i \leqq m$, $d = \bigvee_{x=1}^{m} x$ であることから，$((j-i)\cdot d)$ のどんな素因数も m 以下でなければならない．) したがって $p| \bigvee_{x=1}^{m} x$ すなわち $p|d$ となるが，すると (†) から $p|1$ となって矛盾する．

□

ここで 3 変数関数 β および 1 変数関数 δ, γ を次のように定義する．

$$\beta(x,y,i) = \mathrm{rm}(x,\ (i+1)\cdot y+1).$$

$$\delta(x) = \bigvee_{i=1}^{x} i.\ (\text{ただし } \delta(0)=1 \text{ とする．})$$

$$\gamma(x) = \bigvee_{i=0}^{x} ((i+1)\cdot\delta(x)+1).$$

すると次が成り立つ．

定理 4.24 (β関数定理) $f(x)$ を自然数上の任意の全域関数，n を任意の自然数とし，m を $\{n, f(0), f(1), \cdots, f(n)\}$ の中の最大値とする．すると以下の条件を満たす自然数 a が存在する．

- $a < \gamma(m)$.
- $0 \leqq i \leqq n$ ならば $\beta(a, \delta(m), i) = f(i)$.

[証明] 関数 g を

$$g(i) = (i+1)\cdot\delta(m)+1$$

として，中国剰余定理 (定理 4.22) と補題 4.23 ($n=0$ の時には不要) による．□

さて，

$$\mathrm{h}(x,y) = \frac{(x+y)(x+y+1)}{2} + x,$$

$$\mathrm{left}(z) = \mu x[(\exists y<(z+1))(z=\mathrm{h}(x,y))],$$

$$\mathrm{right}(z) = \mu y[(\exists x<(z+1))(z=\mathrm{h}(x,y))],$$

とすると，自然数のペア $\langle a_0,\ a_1\rangle$ は次の方法で一つの自然数 e にコード化される (?? ページ参照)．

コード化 $e = \mathrm{h}(a_0, a_1)$.

復元 $a_0 = \mathrm{left}(e),\ a_1 = \mathrm{right}(e)$.

ここで先程の関数 β とこれらを使って

$$\mathrm{decode}(e,i) = \beta(\mathrm{left}(e), \mathrm{right}(e), i)$$

という関数 decode を定義すると，自然数の有限列 $a_0, \cdots, a_n$ は以下の方法で

一つの自然数 e にコード化される．

$$\text{コード化}\ e = \mu e[(\forall i \leqq n)(\mathrm{decode}(e,i) = a_i)].$$

$$\text{復元}\ a_i = \mathrm{decode}(e,i).$$

次の定理は，この方法が妥当であること (どんな有限列もコード化されること) を保証している．

定理 4.25 (有限列コード化可能定理) 自然数の任意の有限列 $a_0, \cdots, a_n$ に対して，以下を満たす自然数 e が存在する:

$$0 \leqq i \leqq n \text{ なるすべての } i \text{ に対して } \mathrm{decode}(e,i) = a_i.$$

[証明] $f(0) = a_0, \cdots, f(n) = a_n$ として先程の β関数定理を適用して，得られる m と a を用いて $e = \mathrm{h}(a, \delta(m))$ とすればよい．□

4.6　原始再帰法の消去

この節では前節の結果を使って「初期関数を少しだけ増やせば再帰的全域関数を原始再帰法を使わずに定義できる」ということを証明する．この結果は不完全性定理の証明のための「表現定理」(5.5 節) で必要になる．

自然数上の全域関数のクラス $\mathcal{R}$ を以下の (1)～(3) で再帰的に定義する．

(1) **初期関数**: 足し算 $\mathrm{plus}(x,y)$, 掛け算 $\mathrm{times}(x,y)$, 射影関数 $\mathrm{P}_i^k(x_1, \cdots, x_k)$, および等号の特性関数:

$$\mathrm{equal}(x,y) = \begin{cases} 1, & (x = y \text{ のとき}), \\ 0, & (x \neq y \text{ のとき}), \end{cases}$$

は $\mathcal{R}$ に属す．

(2) **関数合成**: $\mathcal{R}$ に属す関数を合成して得られる関数はまた $\mathcal{R}$ に属す．

(3) **最小化**: $(k+1)$ 変数関数 g が $\mathcal{R}$ に属し，条件「どんな $x_1, \cdots, x_k$ に対しても適当な y をとれば $g(x_1, \cdots, x_k, y) = 0$ になる」が満たされるならば，

$$f(x_1, \cdots, x_k) = \mu y[g(x_1, \cdots, x_k, y) = 0]$$

なる k変数関数 f も $\mathcal{R}$ に属す．

すると 4.1 節の例 3 や 4.2 節の例 5 などから明らかに，$\mathcal{R}$ に属す関数は再帰的である．以下ではこの逆，すなわち任意の再帰的全域関数は $\mathcal{R}$ に属すこと (定理 4.31) を証明する．

補題 4.26 k 変数のゼロ関数 $\mathrm{Z}_k(x_1,\cdots,x_k)=0$, 1 変数の恒等関数 $\mathrm{one}(x)=1$, および後者関数 $\mathrm{S}(x)$ はすべて $\mathcal{R}$ に属す．(したがって任意の恒等関数は $\mathcal{R}$ に属す．)

[証明] $\mathrm{Z}_k(x_1,\cdots,x_k)=\mu y[\mathrm{P}^{k+1}_{k+1}(x_1,\cdots,x_k,y)=0]=\mu y[y=0]$.
$\mathrm{one}(x)=\mu y[\mathrm{equal}(\mathrm{Z}_2(x,y),\mathrm{P}^2_2(x,y))=0]=\mu y[\mathrm{equal}(0,y)=0]$.
$\mathrm{S}(x)=\mathrm{plus}(\mathrm{P}^1_1(x),\mathrm{one}(x))=x+1$. □

特性関数が $\mathcal{R}$ に属すような関係を $\mathcal{R}$ 関係と呼ぶ．

補題 4.27 $\mathcal{R}$ 関係のクラスは否定と連言について閉じている．(したがって選言など他の命題演算についても閉じている．)

[証明] $\chi_{\neg A}=\mathrm{equal}(\chi_A,\mathrm{Z}_k)$. $\chi_{A\wedge B}=\mathrm{times}(\chi_A,\chi_B)$. □

補題 4.28 $\mathcal{R}$ 関係 $A(x_1,\cdots,x_k,y)$ が条件「どんな $x_1,\cdots,x_k$ に対しても適当な y をとれば $A(x_1,\cdots,x_k,y)$ が成り立つ」を満たすならば，

$$f(x_1,\cdots,x_k)=\mu y\ A(x_1,\cdots,x_k,y)$$

なる関数 f は $\mathcal{R}$ に属す．

[証明] $f(x_1,\cdots,x_k)=\mu y[\chi_{\neg A}(x_1,\cdots,x_k,y)=0]$. □

補題 4.29 $A(x_1,\cdots,x_k,y)$ が $\mathcal{R}$ 関係ならば，$x_1,\cdots,x_k,z$ を変数とする関係 $(\exists y<z)A(x_1,\cdots,x_k,y)$ と $(\forall y<z)A(x_1,\cdots,x_k,y)$ は $\mathcal{R}$ 関係である．

[証明] $(\exists y<z)A(x_1,\cdots,x_k,y) \quad\Leftrightarrow\quad \mu y[y=z\ \vee\ A(x_1,\cdots,x_k,y)]\neq z$.
$(\forall y<z)A(x_1,\cdots,x_k,y) \quad\Leftrightarrow\quad \neg(\exists y<z)\neg A(x_1,\cdots,x_k,y)$. □

補題 4.30　4.5 節の関数 h, left, right, rm, β, decode はすべて $\mathcal{R}$ に属す．

[証明]　「2 で割る」関数

$$\mathrm{half}(x) = \mu y[(2 \cdot y = x) \ \vee \ (2 \cdot y + 1 = x)]$$

を用いれば，h, left, right が $\mathcal{R}$ に属することがわかる．また，

$$\mathrm{rm}(x, y) = \mu z[(\exists q < (x+1))(x = q \cdot y + z)]$$

とでき，これらによって β, decode は定義される．□

定理 4.31　任意の再帰的全域関数 f は $\mathcal{R}$ に属す．

[証明]　再帰的全域関数の定義に関する帰納法による．f が Z() や S(x) の場合は補題 4.26 より言える．f が P_i^k の場合や他の関数から合成や最小化で得られる場合は，$\mathcal{R}$ の定義や帰納法の仮定より明らか．f が g, h から原始再帰法で得られる場合を考える．すなわち，

$$f(\overrightarrow{x}, 0) = g(\overrightarrow{x}),$$

$$f(\overrightarrow{x}, (y+1)) = h(\overrightarrow{x}, y, f(\overrightarrow{x}, y)),$$

であるとする ($\overrightarrow{x}$ は $x_1, \cdots, x_k$ を表す)．このとき 4.5 節で示した方法によって有限列

$$f(\overrightarrow{x}, 0), f(\overrightarrow{x}, 1), \cdots, f(\overrightarrow{x}, y)$$

をコード化する関数 $t(\overrightarrow{x}, y)$ は

$$\begin{aligned} t(\overrightarrow{x}, y) \ = \ \mu e[&\mathrm{decode}(e, 0) = g(\overrightarrow{x}) \ \wedge \\ &(\forall i < y)(\mathrm{decode}(e, i+1) = h(\overrightarrow{x}, y, \mathrm{decode}(e, i)))] \end{aligned}$$

となり，今までの補題とコード化可能定理 (定理 4.25) と帰納法の仮定によって $t \in \mathcal{R}$ が示される．そして

$$f(\overrightarrow{x}, y) = \mathrm{decode}(t(\overrightarrow{x}, y), y)$$

となるので，f も $\mathcal{R}$ に属する．□

結局，$\mathcal{R}$ に属す関数によるコード化を用いて原始再帰法を実現したことが，ここでのポイントである．

パート A 参考文献

述語論理の入門書は，日本語でもすでに何十冊も出版されているので，あえてここに紹介するまでもないと思うが，何も情報のない人の取っ掛りとして，比較的新しい本を 2 つあげておく．これ以外にも良書はたくさんある．

[1] 小野寛晰著『情報科学における論理』日本評論社 1994.

[2] 角田譲著『数理論理学入門』朝倉書店 1996.

さて，論理の初歩を勉強したあと，あるいはそれと平行して「数学基礎論」を学ぶとなると適当な本はぐっと少なくなる．次にあげる本 [3]〜[9] は，永く広く読まれてきた名著であり，やや古めかしいところもあるが，もっとも基礎論らしい基礎論の本である．

[3] K. ゲーデル著 (近藤洋逸訳)『数学基礎論 (撰出公理及び一般連続仮説の集合論公理との無矛盾性)』 伊藤書店 1946.

[4] 竹内外史-八杉満利子共著『証明論入門』(『数学基礎論』改題) 共立出版 1988 (初版 1956, 増補版 1974).

[5] P. コーヘン著 (近藤基吉他訳)『連続体仮説』東京図書 1972.

[6] 竹内外史著『数学基礎論の世界』日本評論社 1972.

[7] 倉田令二朗著『数学論序説』ダイヤモンド社 1972.

[8] 前原昭二著『数学基礎論入門』朝倉書店 1977.

[9] D. ヒルベルト・P. ベルナイス (吉田夏彦・渕野昌訳)『数学の基礎』 シュプリンガー・フェアラーク東京 1993.

洋書に関しては，次の 3 冊が評判が高い．[10] は，入門者から専門家まで必携の読める辞典である．[11] は，基礎論の専門家を目指す人が必ず一度は手にする最高級の教科書．現代的な入門書としては [12] を薦めておきたい．

[10] J. Barwise, *Handbook of Mathematical Logic*, North-Holland 1977.

[11] R. Shoenfield, *Mathematical Logic*, Addison-Wesley 1967.

[12] D. van Dalen, *Logic and Structure* (3rd ed.), Springer 1994.

Part B.　不完全性定理

ゲーデルの不完全性定理には「算術の公理系をどのように定めても，そこでは証明も反証もできない命題が必ず存在する」という第一定理と,「算術の公理系をどのように定めても，そこでは自らの無矛盾性を証明することはできない」という第二定理がある．このパートBではこれら二つの不完全性定理に対して現代的な手法を用いたなるべく平易でかつ正確な証明を与えるとともに，その後の関連する研究の一端を紹介していく．

まず第5講では算術の形式体系QとPA(ペアノ算術)を導入し，これらの体系の重要な性質 — Σ_1完全性，再帰的関数の表現可能性など — を証明する．

第一不完全性定理の証明は「この文は証明できない」という意味の文を作ることによって行なわれるが，この構成のための必須の要素が「ゲーデル数」「可証性述語」「対角化定理」である．第6講ではこれらを順に説明して第一定理の証明を与える．

第7講では第一定理のロッサーによる拡張とクレイグの手法による拡張を説明する．また算術や述語論理の決定不能性に関するいくつかの結果を証明する．

第二不完全性定理は第一定理の証明を算術で形式化すれば導かれる．第8講では，この「形式化」がいかに行なわれるかを「可導性条件」という性質を用いて明らかにして第二定理を証明する．さらに関連する結果として，レーブの定理，可証性述語と様相論理との対応などについて説明する．

最後に第9講では可証性述語の詳細な定義を与え，第8講で証明せずに使用した重要な性質(可導性条件)の証明を説明する．

本文中での記号等の使い方について次の二つだけ注意しておく．まず,「≡」は「右辺と左辺が等しい文字列である」を意味する．たとえば論理式 φ と ψ について「$\varphi \equiv \psi$」と書いたら，これは「φ と ψ はまったく同じ論理式である」または「論理式 φ を ψ と定義する」ということである．また，変数などの列 $x_1, x_2, \cdots, x_n$ を $\overrightarrow{x}$ と表記することがある．この場合，論理式 $\forall x_1 \forall x_2 \cdots \forall x_n\, \varphi$ のことを $\forall \overrightarrow{x} \varphi$

とも表記する.

第 5 講　算術の体系

5.1　ロビンソンの算術 Q

不完全性定理は算術の形式体系に関する定理であるので，これをきちんと説明するためには算術の形式体系を具体的に定めてその性質を示しておく必要がある．そこでこの 5.1節と次の 5.2節で Q と PA という二つの算術の形式体系を導入して，後の 5.3〜5.5節で Q や PA のいくつかの重要な性質を明らかにする．

Q はロビンソン (R.M. Robinson) によって与えられた算術の理論であり，第一不完全性定理を説明するための必要最低レベルの能力 — 自然数上の足し算と掛け算に関する基本的な公理だけ — を備えている．具体的には，Q は第 3 講で登場した述語論理の公理 (30 ページの P1〜P6) および推論規則 (三段論法と一般化法則，30 ページの (3) と (4)) に Q の固有の公理を加えた体系である．したがって，Q の言語と Q の固有の公理を定めることによって Q が定義される．

Q で扱う記号は，

定数記号　0

関数記号　$\mathrm{S}, +, \cdot$

と，述語論理の記号 (変数記号 $x, y, z, \cdots$ と等号 $=$ と論理記号 $\neg, \rightarrow, \forall$) である．関数記号 S は 1 変数の後者関数 (すなわち $\mathrm{S}(x) = x + 1$) を意味し，$+$ と $\cdot$ はそれぞれ足し算と掛け算を意味している．そして Q の項，論理式はこれらの記号だけを組み合わせて作られる．自由変数を含まない論理式のことを文と呼ぶ (3.1 節参照)．

ここで Q の項や論理式を記述するいくつかの省略記法を定義しておく．まず論理式 $\perp, \varphi \wedge \psi, \varphi \vee \psi, \varphi \leftrightarrow \psi, \exists x\, \varphi$ はパート A で導入したようにする (6 ページ，31 ページ参照)．Q は述語記号 $<$ を持っていないが，二つの項 a と b に対して a にも b にも現れない変数 x を用いて作られる論理式

$$\exists x(b = \mathrm{S}(x) + a)$$

が「b は a より真に大きい」を意味しているので，$a < b$ はこの論理式の略記とする．さらに t が項，φ が論理式のときに，

$$\forall x < t\, \varphi \equiv \forall x((x < t) \to \varphi),$$

$$\exists x < t\, \varphi \equiv \exists x((x < t) \land \varphi)$$

とする．これらはそれぞれ「t 未満のすべての x に対して φ が成り立つ」「φ が成り立つような t 未満の x が存在する」を意味している．Q には定数記号は 0 しかないので，自然数 0, 1, 2, $\cdots$ を定数項で表現したいときには

$$0, \mathrm{S}(0), \mathrm{S}(\mathrm{S}(0)), \cdots$$

を用いる．これらの項のことを**数項 (numeral)** と呼び，

$$\overline{0}, \overline{1}, \overline{2}, \cdots$$

と表記する．

さて，Q の固有の公理は次の 7 つである．

A1: $\forall x \forall y(\mathrm{S}(x) = \mathrm{S}(y) \;\to\; x = y)$

A2: $\forall x \neg(\mathrm{S}(x) = 0)$

A3: $\forall x(\neg(x = 0) \;\to\; \exists y(x = \mathrm{S}(y)))$

A4: $\forall x(x + 0 = x)$

A5: $\forall x \forall y(x + \mathrm{S}(y) = \mathrm{S}(x + y))$

A6: $\forall x(x \cdot 0 = 0)$

A7: $\forall x \forall y(x \cdot \mathrm{S}(y) = (x \cdot y) + x)$

公理 **A1**〜**A3** は自然数に関するデデキント (R. Dedekind) の公理であり，**A4** と **A5** は足し算の再帰的な定義，**A6** と **A7** は掛け算の再帰的な定義である．

Q における証明の例を見てみよう．たとえば $\overline{1} + \overline{1} = \overline{2}$ は以下の方針で Q において証明できる．

1: $\overline{1} + \mathrm{S}(0) = \mathrm{S}(\overline{1} + 0)$. (公理 **A5** より)

2: $\overline{1} + 0 = \overline{1}$. (公理 **A4** より)

3: $\mathrm{S}(\overline{1} + 0) = \mathrm{S}(\overline{1})$. (2 より)

4: $\overline{1} + \mathrm{S}(0) = \mathrm{S}(\overline{1})$, すなわち $\overline{1} + \overline{1} = \overline{2}$. (1, 3 より)

また，$\neg(\overline{1} + \overline{1} = \overline{4})$ は次のように証明できる．

5: $\neg(\overline{2} = 0)$. (公理 **A2** より)

6: $(\overline{3} = \overline{1}) \rightarrow (\overline{2} = \overline{0})$. (公理 **A1** より)

7: $\neg(\overline{3} = \overline{1})$. (5, 6 より)

8: $(\overline{4} = \overline{2}) \rightarrow (\overline{3} = \overline{1})$. (公理 **A1** より)

9: $\neg(\overline{4} = \overline{2})$. (7, 8 より)

10: $\neg(\overline{1} + \overline{1} = \overline{4})$. (4 と 9 より)

30 ページで定義した意味での「Q における $\overline{1} + \overline{1} = \overline{2}$ の証明」「Q における $\neg(\overline{1} + \overline{1} = \overline{4})$ の証明」は，これらの方針にしたがって作ることができる．Q で論理式 φ が証明できること，証明できないことをそれぞれ

$$\mathrm{Q} \vdash \varphi, \qquad \mathrm{Q} \nvdash \varphi$$

と書く (3.2 節参照)．

Q では上に挙げたような具体的な数値に関する命題ならば証明できるが，変数の入った命題 ($\forall x(\cdots)$ という形の論理式) については証明できないものが多い (たとえば $\mathrm{Q} \nvdash \forall x(0 + x = x)$ である)．Q の能力は「算数の計算問題ならば解けるが，一般化された数学の問題の多くは解けない小学生レベル」と言ってもよいだろう．しかしこのような非常に弱い算術 Q でも，この後で展開していく第一不完全性定理を示すために必要な能力は充分に持っているのである．

5.2　ペアノ算術

次に，通常**ペアノ算術 (Peano Arithmetic)** と呼ばれる算術の形式体系 PA を導入しよう．PA は Q を強めたものであり，第二不完全性定理を説明する際に基本となる理論である．

PA の言語は Q と同じであり，PA の固有の公理は Q の公理 **A1**〜**A7** と次の**帰納法の公理**である．

帰納法の公理 : $\forall \overrightarrow{y}[(\varphi(0, \overrightarrow{y}) \land \forall x(\varphi(x, \overrightarrow{y}) \rightarrow \varphi(\mathrm{S}(x), \overrightarrow{y}))) \rightarrow \forall x\, \varphi(x, \overrightarrow{y})]$

ただし $\varphi(x, \overrightarrow{y})$ は PA の任意の論理式で，$\overrightarrow{y} \equiv y_1, \cdots, y_k (k \geq 0)$ である．この公理はいわゆる数学的帰納法「$A(n)$ がすべての自然数 n に対して成り立つことを示すには，

1. $A(0)$ は成り立つ

2. $A(x)$ が成り立つならば $A(x+1)$ も成り立つ

を示せばよい」を意味している ($\overrightarrow{y}$ を任意に固定して $\varphi(n, \overrightarrow{y})$ を $A(n)$ と考える). なお論理式 $\varphi(x, \overrightarrow{y})$ の取り方は任意なので, PA は Q に無限に多くの公理を加えた体系になる.

PA における証明の例を見てみよう. $\forall x(0+x=x)$ は Q では証明できないが PA では次のような方針で証明できる.

$\varphi(x) \ \equiv \ 0+x=x$ とする.

1: $0+0=0$, すなわち $\varphi(0)$. (公理 **A4** より)

2: $0+x=x \ \rightarrow \ \mathrm{S}(0+x)=\mathrm{S}(x)$.

(等号に関する公理 (30 ページの P5, P6) より)

3: $0+\mathrm{S}(x)=\mathrm{S}(0+x)$. (公理 **A5** より)

4: $0+x=x \ \rightarrow \ 0+\mathrm{S}(x)=\mathrm{S}(x)$, すなわち $\varphi(x) \ \rightarrow \ \varphi(\mathrm{S}(x))$.

(2, 3 と等号に関する公理より)

5: $\forall x\varphi(x)$. (1, 4 と帰納法の公理より)

また, PA では Q の公理 **A3** を他の公理から次のように導くことができるので, **A3** は公理としては不要になる.

$\varphi(x) \ \equiv \ \neg(x=0) \ \rightarrow \ \exists y(x=\mathrm{S}(y))$ とする.

1: $0=0$. (等号に関する公理より)

2: $\neg(0=0) \ \rightarrow \ \exists y(0=\mathrm{S}(y))$, すなわち $\varphi(0)$. (1 より)

3: $\mathrm{S}(x)=\mathrm{S}(x)$. (等号に関する公理より)

4: $\exists y(\mathrm{S}(x)=\mathrm{S}(y))$. (3 より)

5: $\neg(\mathrm{S}(x)=0) \ \rightarrow \ \exists y(\mathrm{S}(x)=\mathrm{S}(y))$, すなわち $\varphi(\mathrm{S}(x))$. (4 より)

6: $\forall x(\varphi(x) \ \rightarrow \ \varphi(\mathrm{S}(x)))$. (5 より)

7: $\forall x\varphi(x)$. (2, 6 と帰納法の公理より)

このように PA では帰納法の公理を用いることによって Q で証明できなかった $\forall x(\cdots)$ という形の多くの論理式が証明でき, かなり複雑な論理式も証明できるようになる. しかし自然数のすべての性質が PA で証明できるわけではない. そし

てこのことは不完全性定理によって示されるのである．

5.3 Q の基本的な能力

この節では，今後必要になる Q のいくつかの基本的な証明能力を示しておく．5.1節で「Q では $\forall x(\cdots)$ という形の多くの論理式が証明できない」と述べたが，ここに挙げる定理 5.2や定理 5.3(d) は，Q で証明できる $\forall x(\cdots)$ という形の論理式の典型的な例を示している．

定理 5.1　(1) n と m が異なる自然数であるならば，$\mathrm{Q} \vdash \neg(\overline{n} = \overline{m})$.

(2) 任意の自然数 n, m に対して，$\mathrm{Q} \vdash \overline{n} + \overline{m} = \overline{n+m}$.

(3) 任意の自然数 n, m に対して，$\mathrm{Q} \vdash \overline{n} \cdot \overline{m} = \overline{n \cdot m}$.

(4) t が変数を含まない項 (すなわち 0, S, +, · のみで構成される項)，n が $\mathfrak{N} \models t = \overline{n}$ なる自然数ならば，$\mathrm{Q} \vdash t = \overline{n}$ である (ただし $\mathfrak{N}$ は算術の標準モデル (3.1 節参照))．

[証明]　(1) は 5.1節の Q における証明の方針中の

$$9 : \neg(\overline{4} = \overline{2})$$

と同様にできる．(2) と (3) は m に関する数学的帰納法により，(4) は t の構成に関する帰納法により，それぞれ示される．□

注意.　たとえば (2) の証明を正確に言うと，n を任意に固定した自然数として，そのとき m に関する数学的帰納法によって

どんな m に対しても $\mathrm{Q} \vdash \overline{n} + \overline{m} = \overline{n+m}$ が成り立つ

ことを示すのである．この数学的帰納法は形式体系の性質を論じる立場での数学的帰納法であり，PA が体系の中に持っている帰納法の公理とは使用のレベルが異なることを確認されたい．

定理 5.2　(1) $\mathrm{Q} \vdash \forall x\, \neg(x < 0)$.

(2) 任意の自然数 n に対して，$\mathrm{Q} \vdash \forall x(x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n} \vee \overline{n} < x)$.

(3) 任意の自然数 n に対して，$\mathrm{Q} \vdash \forall x < \overline{n+1}(x = 0 \vee x = \overline{1} \vee \cdots \vee x = \overline{n})$.

[証明] (2) の証明だけを行なう ((1)(3) も難しくはない)．次の (2-1)(2-2) から数学的帰納法によって (2) は導かれる．

(2-1) $\mathrm{Q} \vdash \forall x(x = 0 \vee 0 < x)$.

(2-2) 任意の m に対して $\mathrm{Q} \vdash \forall x(\overline{m} < x \ \rightarrow \ (x = \overline{m+1} \vee \overline{m+1} < x))$.

(2-1) は公理 **A3**, **A4** により示される．(2-2) は次の推論を Q の中で行えばよい：$\overline{m} < x$ を仮定する．すなわちある y について $x = \mathrm{S}(y) + \overline{m}$ であるとする．ここで (2-1) により $y = 0 \vee 0 < y$ である．もし $y = 0$ ならば $x = \mathrm{S}(0) + \overline{m}$ となるが，これを公理 **A4**, **A5** を使って変形すれば $x = \overline{m+1}$ になる．もし $0 < y$ ならば，ある z について $y = \mathrm{S}(z) + 0$ ということになり，$x = \mathrm{S}(\mathrm{S}(z) + 0) + \overline{m}$ となるが，これから公理 **A4**, **A5** を使うと $x = \mathrm{S}(z) + \overline{m+1}$，すなわち $\overline{m+1} < x$ を得る．□

論理式 $\varphi(x)$ に対して，論理式 $\tilde{\varphi}(x)$ を

$$\tilde{\varphi}(x) \ \equiv \ \varphi(x) \wedge \forall y {<} x \neg\varphi(y)$$

(ただし y は $\varphi(x)$ に現れない変数) と定義する．

定理 5.3　$\varphi(x)$ を任意の論理式，n を任意の自然数とする．いま，

(a) $\mathrm{Q} \vdash \varphi(\overline{n})$,

(b) $m < n$ なるすべての m に対して $\mathrm{Q} \vdash \neg\varphi(\overline{m})$,

であるならば，

(c) $\mathrm{Q} \vdash \tilde{\varphi}(\overline{n})$,

(d) $\mathrm{Q} \vdash \forall x(\neg(x = \overline{n}) \ \rightarrow \ \neg\tilde{\varphi}(x))$,

である．

[証明] (c):　$n = 0$ の場合は定理 5.2(1) と (a) より明らか．$n \geq 1$ の場合は，(b) より

$$(\dagger) \quad \mathrm{Q} \vdash \forall y((y = \overline{0} \vee y = \overline{1} \vee \cdots \vee y = \overline{n-1}) \ \rightarrow \ \neg\varphi(y))$$

となり，定理 5.2(3) と (a) を使って $\mathrm{Q} \vdash \tilde{\varphi}(\overline{n})$ が示される．

(d): 条件 (a) より

$$\mathrm{Q} \vdash \overline{n} < x \ \rightarrow \ \exists y(y < x \wedge \varphi(y))$$

となり，これと (†) と定理 5.2(2) によって

$$\mathrm{Q} \vdash \forall x(\neg\varphi(x) \vee x = \overline{n} \vee \exists y(y < x \wedge \varphi(y)))$$

となり (d) が示される．□

5.4　Σ_1完全性定理

ここでは Σ_1, Π_1, Δ_1 (それぞれシグマワン，パイワン，デルタワンと読む) という論理式の種類を定め，Q の重要な性質 (Σ_1完全性定理) を証明する．Σ_1論理式や Δ_1論理式は，特に第 8 講や第 9 講で第二不完全性定理を証明する際に重要な役割を果たすことになる．

定義. 「φ は理論 T 上の Σ_1論理式である」ということを以下の (1)〜(3) で再帰的に定義する．

(1) φ が $s = t$, $\neg(s = t)$ (ただし s, t は項) のいずれかの形をしているならば，これは T 上の Σ_1論理式である．

(2) φ が $\varphi' \wedge \varphi''$, $\varphi' \vee \varphi''$, $\exists x\, \varphi'$, $\forall x < t\, \varphi'$ (ただし t は変数 x を含まない項) のいずれかの形をしていて，φ' と φ'' が T 上の Σ_1論理式であるならば，φ も T 上の Σ_1論理式である．

(3) T 上の Σ_1論理式 ψ が存在して $T \vdash \varphi \leftrightarrow \psi$ となるならば，φ も T 上の Σ_1論理式である．

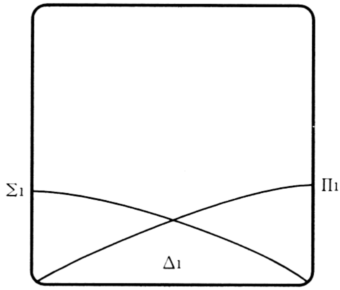
定義. 理論 T 上の Π_1論理式と Δ_1論理式を次のように定義する．

φ は T 上のΠ_1論理式である $\Leftrightarrow$ T 上のΣ_1論理式 ψ が存在して $T \vdash \varphi \leftrightarrow \neg\psi$ となる．

φ は T 上の Δ_1論理式である $\Leftrightarrow$ φ は T 上の Σ_1論理式かつ T 上の Π_1論理式である．

さらに，自由変数を含まない Σ_1, Π_1, Δ_1論理式のことをそれぞれ Σ_1文，Π_1文，Δ_1文とも呼ぶ．

論理式全体



定理 5.4 (Σ_1完全性定理) T は Q に公理を加えて得られる理論で，$\mathfrak{N}$ をモデルとして持つものとする．このとき，φ が T 上のΣ_1文で $\mathfrak{N} \models \varphi$ であるならば $T \vdash \varphi$ である．すなわち，正しい Σ_1文は T で証明できる．

この定理は次の補題の特別な場合になるので，補題を示すことにより証明は完了する．

補題 5.5 論理式 φ の自由変数に数項を代入して得られる文のことを φ の代入結果と呼ぶことにする．T を上と同じ理論とし，φ を T 上の任意の Σ_1論理式とする．このとき，文 φ^* が φ の代入結果で $\mathfrak{N} \models \varphi^*$ であるならば $T \vdash \varphi^*$ である．
[証明] 「φ が T 上の Σ_1論理式である」ことの定義に関する帰納法による．φ が $s = t$ または $\neg(s = t)$ という形のときは，定理 5.1により簡単に示される．φ が $\varphi' \land \varphi''$ または $\varphi' \lor \varphi''$ または $\exists x\, \varphi'(x)$ のときは，帰納法の仮定より明らか．φ が $\forall x < t\, \varphi'(x)$ のとき：いま，φ から φ^* を得る代入と同じ代入を論理式 ψ に施した結果を ψ^* と表記することにする．n を $\mathfrak{N} \models (t = \overline{n})^*$ なる自然数とすると帰納法の仮定から，n 未満のすべての m に対して $T \vdash (\varphi'(\overline{m}))^*$ となり，定理 5.3の (c) と同様に $T \vdash (\forall x < t\, \varphi'(x))^*$ を得る．最後に，T上のΣ_1論理式 ψ に対

して $T \vdash \varphi \leftrightarrow \psi$ となるときは，帰納法の仮定と $T \vdash \varphi^* \leftrightarrow \psi^*$, $\mathfrak{N} \models \varphi^* \leftrightarrow \psi^*$ より明らか．□

注意.

(1) σ と σ' が T 上の Σ_1論理式，π と π' が T 上の Π_1論理式，δ と δ' が T 上の Δ_1論理式のときには次が成り立つ．

- $\sigma \wedge \sigma'$, $\sigma \vee \sigma'$, $\forall x < t\, \sigma$, $\exists x < t\, \sigma$, $\exists x\, \sigma$ はすべて T 上の Σ_1論理式であるが，$\neg\sigma$, $\forall x \sigma$ は一般にそうではない．また，$\neg\sigma$ は T 上の Π_1論理式である．
- $\pi \wedge \pi'$, $\pi \vee \pi'$, $\forall x < t\, \pi$, $\exists x < t\, \pi$, $\forall x\, \pi$ はすべて T 上の Π_1論理式であるが，$\neg\pi$, $\exists x \pi$ は一般にそうではない．また，$\neg\pi$ は T 上の Σ_1論理式である．
- $\delta \wedge \delta'$, $\delta \vee \delta'$, $\neg\delta$, $\forall x < t\, \delta$, $\exists x < t\, \delta$ はすべて T 上の Δ_1論理式であるが，$\forall x\, \delta$, $\exists x\, \delta$ は一般にそうではない．

(2) Σ_1完全性定理の「Σ_1文」を「Π_1文」に変えた命題は一般には成り立たない．たとえば $T = \mathrm{Q}$ のときには $\forall x(0 + x = x)$ が Q で証明できないし，$T = \mathrm{PA}$ になっても「$\mathfrak{N} \models \varphi$ かつ $\mathrm{PA} \nvdash \varphi$」なる Π_1文 φ が存在することが不完全性定理によって示される．

(3) 「T 上の Σ_1・Π_1・Δ_1論理式」の定義は理論 T の証明能力に依存するので，正確に述べるときには「T 上の」という言葉を落してはいけない．しかし T の違いが重要でないときや T が文脈から明らかなときには，単に「Σ_1・Π_1・Δ_1論理式」と書くこともある．

(4) 本書の他のパートや他の文献に登場する Σ_1, Π_1, Δ_1 (あるいは Σ^0_1, Π^0_1, Δ^0_1) とここで定義した Σ_1, Π_1, Δ_1 とは，微妙に異なる場合もあるが本質的には同じものである．たとえばある論理式 φ が一方の定義では Σ_1, もう一方の定義ではそうでない，ということがあるが，この場合は φ と同等な論理式でどちらの定義でも Σ_1 になるもの考えればよい．

5.5 表現可能性

この節では「再帰的関数は Q において Σ_1論理式で表現できる」「原始再帰的関数は PA において Δ_1論理式 (ならびに関数記号) で表現できる」ということを説明する．これらは Q や PA の非常に重要な性質であり，第 6 講以降で頻繁に用いられることになる．

定義．自然数上の関係や関数が算術の理論において「表現 **(represent)** される」「表現可能 **(representable)** である」ということを次の (1)(2) で定義する．

(1) $R(\overrightarrow{n})$ を自然数上の k 項関係とし，T を算術の理論とし，$\varphi(\overrightarrow{x})$ を $x_1, \cdots, x_k$ 以外には自由変数を含まない論理式とする．いま，任意の自然数 $n_1, \cdots, n_k$ に対して

- $R(n_1, \cdots, n_k)$ が成り立つときには $T \vdash \varphi(\overline{n_1}, \cdots, \overline{n_k})$
- $R(n_1, \cdots, n_k)$ が成り立たないときには $T \vdash \neg\varphi(\overline{n_1}, \cdots, \overline{n_k})$

が満たされるならば,「関係 $R(\overrightarrow{n})$ は理論 T において論理式 $\varphi(\overrightarrow{x})$ によって表現される」と言う．また，このような論理式 $\varphi(\overrightarrow{x})$ が存在するときに,「関係 R は理論 T において表現可能である」と言う．

(2) f を自然数上の k 変数全域関数とし，T を算術の理論とし，$\varphi(\overrightarrow{x}, y)$ を $x_1, \cdots, x_k, y$ 以外には自由変数を含まない論理式とする．いま，$(k+1)$ 項関係

$$f(n_1, \cdots, n_k) = n_{k+1}$$

が T において $\varphi(x_1, \cdots, x_k, x_{k+1})$ によって表現され，

$$T \vdash \forall y\, \forall y' ((\varphi(\overline{n_1}, \cdots, \overline{n_k}, y) \land \varphi(\overline{n_1}, \cdots, \overline{n_k}, y')) \ \rightarrow\ y = y')$$

が任意の自然数 $n_1, \cdots, n_k$ に対して成り立つならば,「関数 $f(\overrightarrow{n})$ は理論 T において論理式 $\varphi(\overrightarrow{x}, y)$ によって表現される」と言う．また，このような論理式 $\varphi(\overrightarrow{x}, y)$ が存在するときに「関数 f は理論 T において表現可能である」と言う．

注意. 文献によってはここで単に表現可能と呼んだ性質を「**数値別 (numeralwise) に表現可能**」と呼ぶ場合がある．そしてこの言葉に込められた次の意図に注意する必要がある：たとえば上の (1) では，自由変数に数項を代入して得られる文 $\varphi(\overline{n_1},\cdots,\overline{n_k})$ や $\neg\varphi(\overline{n_1},\cdots,\overline{n_k})$ の証明可能性だけが問題になっているのであって，変数のままの $\varphi(\overrightarrow{x})$ という論理式の証明可能性には一切言及していない．一般に，理論 T において論理式 $\varphi(x)$ が関係 $R(n)$ を表現し，$R(n)$ がすべての自然数 n に対して成り立つならば，すべての n について $T\vdash\varphi(\overline{n})$ である．ところがこの時 $T\vdash\forall x\varphi(x)$ とは限らない．

定理 5.6 (再帰的全域関数・再帰的関係の表現定理) (1) Q において表現可能な全域関数や関係は，すべて再帰的である．
(2) 任意の再帰的全域関数，任意の再帰的関係は，Q 上の適当な Σ_1論理式，ならびに適当な Π_1論理式で Q において表現される．(したがって Q に公理を加えたどんな理論 T においても同様に表現可能である．)

この定理により「再帰的全域関数，再帰的関係」「Q において表現可能な全域関数，関係」「Q において Σ_1論理式によって表現される全域関数，関係」「Q において Π_1論理式によって表現される全域関数，関係」のクラスはすべて一致することが言える．

さて，この定理の (1) は以下の議論により示される： たとえば k 変数関数 f が Q において $\varphi(\overrightarrow{x},y)$ によって表現されているとする．このとき，与えられた自然数 $\overrightarrow{n}$ に対する関数値 $f(\overrightarrow{n})$ を計算するには,「Q における証明」をしらみつぶしに検索して

$$\varphi(\overline{n_1},\cdots,\overline{n_k},\overline{m})$$

という形の論理式の証明を見つけ，この m を答とすればよい．このような証明が必ず見つかること，および $m'\neq m$ なる m' に対しては $\varphi(\overline{n_1},\cdots,\overline{n_k},\overline{m'})$ の証明は存在しないことは,「表現される」ということの定義と Q が無矛盾であることから保証される．

また (2) は，関数についての表現可能性が示されれば関係の表現可能性はその特性関数の表現可能性から簡単に示される (論理式 $\varphi(\overrightarrow{x},\overline{1})$ を考えればよい).

したがって以下では再帰的全域関数の表現可能性を証明する.

まず関数の表現可能性が別の形で定義できることを示しておこう.

補題 5.7 関数 $f(\overrightarrow{x})$ が Q において論理式 $\varphi(\overrightarrow{x},y)$ によって表現されるということは，以下の条件と同値である： 任意の自然数 $n_1,\cdots,n_k$ に対して

$$\mathrm{Q}\vdash\forall y(y=\overline{f(\overrightarrow{n})}\ \leftrightarrow\ \varphi(\overline{n_1},\cdots,\overline{n_k},y))$$

が成り立つ.

この補題の証明はそれほど難しくないので省略する.

定理 5.8 (再帰的全域関数の表現定理) 任意の再帰的全域関数は，Q 上の適当な Σ_1論理式ならびに適当な Π_1論理式によって，Q において表現される.

[証明] 任意の再帰的全域関数は 4.6節で与えたクラス $\mathcal{R}$ の要素である (定理 4.31). したがって,「$f\in\mathcal{R}$ なる任意の k 変数関数 f に対して，自由変数を $x_1,\cdots,x_k,y$ 以外には含まず先程の補題 5.7の条件を満たす Σ_1論理式 $\varphi^{\Sigma}(\overrightarrow{x},y)$ と Π_1論理式 $\varphi^{\Pi}(\overrightarrow{x},y)$ が存在する」ことを，$\mathcal{R}$ の定義に関する帰納法によって証明すればよい：f が初期関数 plus, times, p_i^k, equal のときには，φ^{Σ} と φ^{Π} はそれぞれ次の論理式にする.

$$y=x_1+x_2,\quad y=x_1{\cdot}x_2,\quad y=x_i,$$

$$((x_1=x_2)\wedge(y=\overline{1}))\vee(\neg(x_1=x_2)\wedge(y=\overline{0})).$$

これらはすべて Σ_1 かつ Π_1 である. f が $g_1,\cdots,g_l$ と h から関数合成で得られた場合には，g_i に対して帰納法の仮定により得られる論理式を ψ_i^{Σ}, ψ_i^{Π} とし，h に対して帰納法の仮定により得られる論理式を χ^{Σ}, χ^{Π} とすると，求める φ^{Σ} と φ^{Π} はそれぞれ

$$\exists\overrightarrow{y}[\psi_1^{\Sigma}(\overrightarrow{x},y_1)\wedge\psi_2^{\Sigma}(\overrightarrow{x},y_2)\wedge\cdots\wedge\psi_l^{\Sigma}(\overrightarrow{x},y_l)\wedge\chi^{\Sigma}(\overrightarrow{y},y)],$$

$$\forall\overrightarrow{y}[(\psi_1^{\Sigma}(\overrightarrow{x},y_1)\wedge\psi_2^{\Sigma}(\overrightarrow{x},y_2)\wedge\cdots\wedge\psi_l^{\Sigma}(\overrightarrow{x},y_l))\ \rightarrow\ \chi^{\Pi}(\overrightarrow{y},y)]$$

とすればよい．f が g から最小化で得られた場合には，g に対して帰納法の仮定によって得られる論理式を ψ^{Σ}, ψ^{Π} とすると，求める φ^{Σ} と φ^{Π} はそれぞれ

$$\psi^{\Sigma}(\overrightarrow{x}, y, 0) \wedge \forall z < y \, \neg\psi^{\Pi}(\overrightarrow{x}, z, 0),$$

$$\psi^{\Pi}(\overrightarrow{x}, y, 0) \wedge \forall z < y \, \neg\psi^{\Sigma}(\overrightarrow{x}, z, 0)$$

(ただし z は $\psi^{\Sigma}(\overrightarrow{x}, y, 0)$, $\psi^{\Pi}(\overrightarrow{x}, y, 0)$ に現れない変数) とすればよい．以上の φ^{Σ} と φ^{Π} が先程の補題 5.7の条件を満たすことは，5.3節で挙げた Q の性質などによって示される (たとえば最小化の場合に定理 5.3と同様な証明を行なう)．□

さて，理論が PA になって関数が原始再帰的になるとさらに強い次の事実が知られている．

定理 5.9 (原始再帰的関数の PA での表現定理) 任意の原始再帰的関数 $f(\overrightarrow{n})$ に対して，以下の条件を満たす論理式 $\varphi(\overrightarrow{x}, y)$ が存在する．

- 論理式 $\varphi(\overrightarrow{x}, y)$ は PA で関数 $f(\overrightarrow{n})$ を表現する．
- $\varphi(\overrightarrow{x}, y)$ は PA 上で Δ_1 である．
- $\mathrm{PA} \vdash \forall \overrightarrow{x} \, \exists! y \, \varphi(\overrightarrow{x}, y)$. (この論理式は「各 $\overrightarrow{x}$ に対して $\varphi(\overrightarrow{x}, y)$ を満たす y がそれぞれ唯一存在する」ことを意味するものである．定義は 38 ページ参照．)

[証明の方針] 原始再帰的関数の定義に関する帰納法による．f が Z や S や P^k_i のときは明らか．f が合成で得られたときには先程の定理 5.8の証明と同様にすればよい．この際，

$$\mathrm{PA} \vdash \forall \overrightarrow{x} \, \exists! y \, \psi_i(\overrightarrow{x}, y)$$

(ただし $i = 1, \cdots, l$) ならば，

$$(\dagger) \quad \mathrm{PA} \vdash \exists \overrightarrow{y} (\psi_1(\overrightarrow{x}, y_1) \wedge \psi_2(\overrightarrow{x}, y_2) \wedge \cdots \wedge \psi_l(\overrightarrow{x}, y_l) \wedge \chi(\overrightarrow{y}, y)) \leftrightarrow$$
$$\forall \overrightarrow{y} ((\psi_1(\overrightarrow{x}, y_1) \wedge \psi_2(\overrightarrow{x}, y_2) \wedge \cdots \wedge \psi_l(\overrightarrow{x}, y_l)) \rightarrow \chi(\overrightarrow{y}, y))$$

であることに注意する．f が原始再帰法で得られた場合は定理 4.31の証明で示した方法で関数 decode などを使って φ を定義すればよい．その際，decode などが PA の関数記号として扱えること，ならびに「任意の有限列に対してそのコードが

存在すること」が PA で証明可能であることが必要になるが，これらは 9.1節での議論によって示されることになる．□

注意．この定理と系 3.11とその直後の議論によって，PA にはすべての原始再帰的関数に対する関数記号とそれらに関する公理が入っていると考えてもよい (たとえば関数 $f(\overrightarrow{n})$ が論理式 $\varphi(\overrightarrow{x},y)$ で表現されるならば公理

$$\forall\overrightarrow{x}\,\forall y\,(\varphi(\overrightarrow{x},y)\ \leftrightarrow\ f(\overrightarrow{x})=y)$$

を入れる)．特に系 3.11の直後で議論された論理式の変換 ψ^{-f} については，φ と ψ がともに Δ_1 ならば上の証明中の (†) と同じ議論によって ψ^{-f} も Δ_1 になることがわかる．

第 6 講　第一不完全性定理

6.1　第一不完全性定理の主張 (1)

第一不完全性定理が述べていることを簡単に説明しよう．

定義．条件「理論 T の任意の文 φ について，$T \vdash \varphi$ か $T \vdash \neg\varphi$ のどちらかは成り立つ」が満たされているとき T は完全 (**complete**) であると言い，そうでないとき不完全 (**incomplete**) であると言う．

さて理論 Q は不完全である．不完全であるということは「証明も反証もできない文がある」ということであり，算術を展開するための必要な公理が Q の公理だけでは不足しているということである．それでは，どのような公理を加えれば完全な理論になるだろうか？　帰納法の公理を加えて PA にしたら完全になるだろうか？　否，後で示されるように PA も不完全である．では PA にさらにどんな公理を加えれば完全になるだろうか？　そもそも完全な理論なんてあるのだろうか？

完全な理論が存在することは次の例からわかる：自然数に関するすべての正しい文 (すなわち $\mathfrak{N} \models \varphi$ なるすべての文 φ) を公理とする理論は完全である．しかし実際にこの理論で数学を展開しようと思うと，「$\mathfrak{N} \models \varphi$ なるすべての文 φ を公理とする」という情報だけでは具体的には何がこの理論の公理なのかわからないので，このままでは使えない．

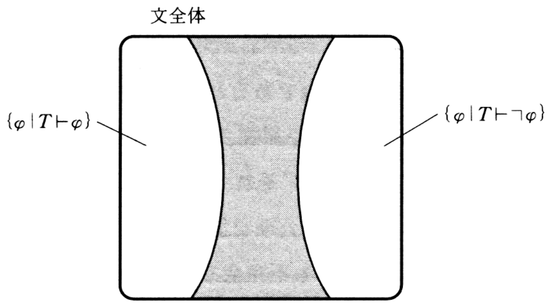
このようなことを考えると，ある理論が数学として妥当であるためにはその公理の集合が再帰的であること — すなわち与えられた文がその理論の公理になっているか否かの判定が機械的にできること — が最低限要請されることがわかる．数学の証明は，もしそれが細部にわたって省略せずに書かれたものならば，その証明に誤りがないことを機械的にチェックできるはずである．ところが公理の集合が再帰的でない場合にはそれができなくなってしまう．

もう一つ，理論が数学として妥当であるために当然要求される条件は無矛盾性で

あろう．矛盾する理論では何でも証明できてしまうので，数学として意味がない．

ところが Q にいくら公理を加えても，これらの二条件 (つまり再帰的な公理化可能性と無矛盾性) を満たしている限りはどうやっても完全な理論になることはできない，という事実を明らかにしたのがゲーデル・ロッサーの第一不完全性定理である．

Q の公理は自然数の最も基本的な性質を表現しており，自然数を扱うことができる数学の理論は必ず Q の公理を含んでいると考えてよい．したがって第一不完全性定理は「自然数を扱うことができるどんな数学の理論にも，そこでは証明も反証もできない命題が必ず存在する」と言っているのである．



T が不完全だと証明も反証もできない文 () がある．

6.2 ゲーデル数

ここで不完全性定理の証明のひとつの重要なアイデアであるゲーデル数を導入する．ゲーデル数は算術の形式体系の「項」や「論理式」などを自然数にコード化した数 (およびそのコード化の方法) であり，これを用いることによって算術の形式体系に関する議論を自然数に関する議論に変えることができる，というのがポイントである．

Q のすべての項，論理式に対して，それぞれ一意に自然数を割り当てる方法を定める．項 t や論理式 φ に割り当てられる自然数のことを項 t のゲーデル数，論理式 φ のゲーデル数と呼び，それぞれ

$$\ulcorner t \urcorner, \ulcorner \varphi \urcorner$$

と表記することにする．ゲーデル数の具体的な定義は後で述べることにして，はじめにゲーデル数の持つ重要な性質を挙げておこう：

- 異なる項，異なる論理式はそれぞれ異なるゲーデル数を持つ．
- 与えられた項や論理式からそのゲーデル数を計算するアルゴリズムがある．
- 与えられた自然数に対して，それが項や論理式のゲーデル数になっているか否かを判定し，もしなっているならその項や論理式を求めるアルゴリズムがある．
- 論理式や項に対するさまざまな操作が，ゲーデル数を用いて自然数上の原始再帰的関数として実現できる．たとえば「論理式 $\forall x\,\varphi(x)$ と 項 t から論理式 $\varphi(t)$ を得る」ということに対しては，次の関数 f がこれを実現する関数である．

$$f(m,n)=\begin{cases}\ulcorner\varphi(t)\urcorner, & (m=\ulcorner\forall x\,\varphi(x)\urcorner, n=\ulcorner t\urcorner \text{ となる}\\ & \quad\text{論理式 } \varphi(x) \text{ と項 } t \text{ が存在するとき}),\\ 0, & (\text{そうでないとき}).\end{cases}$$

(ただし 0 はどんな論理式のゲーデル数でもないとする．)

それではゲーデル数を実際に定義しよう．

まず 8 ページの関数 h を使って関数 $\mathrm{pair}(m,n)$ を

$$\mathrm{pair}(m,n)=2\cdot\mathrm{h}(m,n)=(m+n)(m+n+1)+2m$$

と定義する．これは (自然数 × 自然数) から偶数への全単射である．

Q の項は定数記号 (0) と可算無限個存在する変数記号 $(x,y,z,\cdots)$ から，関数記号 $(\mathrm{S},+,\cdot)$ によって再帰的に定義されていた．そこでその定義にしたがって再帰的に項のゲーデル数を定義する．まず，定数記号と変数記号のゲーデル数は 15 以上の奇数を順に割り当てる：

$$\ulcorner 0\urcorner=15,\quad \ulcorner x\urcorner=17,\quad \ulcorner y\urcorner=19,\quad \ulcorner z\urcorner=21,\cdots$$

関数記号 S, +, · で構成される項に対しては，次のように再帰的に定義する：a と b が項のとき，

$$\ulcorner \mathrm{S}(a)\urcorner=\mathrm{pair}(1,\ulcorner a\urcorner),$$

$$\ulcorner a+b\urcorner=\mathrm{pair}(3,\mathrm{pair}(\ulcorner a\urcorner,\ulcorner b\urcorner)),$$

$$\ulcorner a \cdot b \urcorner = \mathrm{pair}(5, \mathrm{pair}(\ulcorner a \urcorner, \ulcorner b \urcorner)).$$

同様に論理式のゲーデル数も再帰的に定義する：a と b が項のとき，

$$\ulcorner a = b \urcorner = \mathrm{pair}(7, \mathrm{pair}(\ulcorner a \urcorner, \ulcorner b \urcorner)).$$

φ と ψ が論理式で x が変数のとき，

$$\ulcorner \neg\varphi \urcorner = \mathrm{pair}(9, \ulcorner \varphi \urcorner),$$

$$\ulcorner \varphi \to \psi \urcorner = \mathrm{pair}(11, \mathrm{pair}(\ulcorner \varphi \urcorner, \ulcorner \psi \urcorner)),$$

$$\ulcorner \forall x \varphi \urcorner = \mathrm{pair}(13, \mathrm{pair}(\ulcorner x \urcorner, \ulcorner \varphi \urcorner)).$$

(ここでは $\neg$, $\to$, $\forall$ 以外の論理記号はこれらから定義される略記であるとしている．)

以上がゲーデル数の定義である．簡単な例をひとつ計算してみよう：

$$\ulcorner 0 = 0 \urcorner = \mathrm{pair}(7, \mathrm{pair}(15, 15)) = 936070.$$

このように形式体系の構成要素 (項や論理式) と自然数を重複なく対応させることによって，形式体系に関する議論を自然数に関する議論に変えてしまうことが，不完全性定理のひとつの重要なアイデアなのである．

6.3 第一不完全性定理の主張 (2)

6.1節では第一不完全性定理の主張を簡単に説明したが，ここでは算術の理論に関するいくつかの概念を定義しながらこの定理の内容を正確に説明しよう．

はじめに算術の理論に関する「矛盾」「ω (オメガ) 矛盾」といった概念を定義する．

定義．次の (1)(2) を同時に満たす論理式 φ が存在するとき理論 T は**矛盾 (inconsistent)** すると言い，このような φ は存在しないとき T は**無矛盾 (consistent)** であると言う．

(1) $T \vdash \varphi$.

(2) $T \vdash \neg\varphi$.

定義．次の (1)(2) を同時に満たす論理式 $\varphi(x)$ が存在するとき理論 T は **ω矛盾**

(ω-inconsistent) すると言い，このような $\varphi(x)$ は存在しないとき T は ω**無矛盾 (ω-consistent)** であると言う．

(1) $T \vdash \exists x \varphi(x)$.

(2) すべての自然数 n に対して $T \vdash \neg\varphi(\overline{n})$.

ところで，T が矛盾するということは次の 2 条件とそれぞれ同値である (19 ページ，31 ページ参照)：

(a) $T \vdash \bot$.

(b) すべての論理式 φ について $T \vdash \varphi$.

つまり矛盾する理論は「何でも証明できる理論」であり，いかなるモデルも持つことができず (完全性定理 (定理 3.5) 参照)，意味のない理論と言えよう．一方 ω 矛盾する理論は「$\varphi(x)$ を満たす x がある」と言いながら同時に「$\varphi(0)$, $\varphi(1)$, $\varphi(2), \cdots$ は成り立たない」と言っているのであり，$\mathfrak{N}$ をモデルとして持つことができない不自然な理論である．しかし ω矛盾は単なる矛盾とは異なる．上の条件 (b) より明らかに

T が矛盾するならば T は ω矛盾する

(したがって，T が ω無矛盾ならば T は無矛盾)

である．しかしこの逆は必ずしも成り立たない．実際，無矛盾ではあるが ω矛盾している理論が存在する (定理 6.5).

もう少し定義を行なおう．

定義．理論 T_1 の公理が理論 T_0 の公理をすべて含んでいるとき T_1 は T_0 の**拡大 (extension)** であると言う．

たとえば PA は Q の拡大である．

定義．理論 T に対して自然数上の 1 項関係 $\mathbf{Axiom}_T$ を

$$\mathbf{Axiom}_T(n) \Leftrightarrow n \text{ は } T \text{ の固有の公理のゲーデル数である}$$

と定める．そして，この $\mathbf{Axiom}_T$ が再帰的関係であるとき T は**再帰的公理化可能** (recursively axiomatizable) と言い，RE 関係 (すなわち再帰的枚挙可能関係) であるとき T は **RE 公理化可能** (r.e. axiomatizable) であると言う．

たとえば Q の固有の公理は有限個 (7 個) なので Q は再帰的公理化可能である．また PA の固有の公理は無限個だが，公理の形が定まっていて再帰的公理化可能である．

定義． 理論 T の拡大であって再帰的公理化可能な理論のことを T の**再帰的拡大**と言い，RE 公理化可能な理論のことを **RE 拡大**と言う．

たとえば PA は Q の再帰的拡大である．

以上の言葉を使って第一不完全性定理を正確に述べることができる．まずゲーデルの第一不完全性定理は「理論 T が Q の再帰的拡大で ω無矛盾ならば，T は不完全である」であり，これを 6.6節で証明する．さらにこの定理の前提条件である「再帰的拡大」を「RE 拡大」に,「ω無矛盾」を単なる「無矛盾」に，それぞれ弱めることができる．すなわち第一不完全性定理は「理論 T が Q の RE 拡大で無矛盾ならば，T は不完全である」と拡張されるが，これは第 7 講で証明する．

これら第一不完全性定理の証明はいずれも

$$T \nvdash \varphi, \quad T \nvdash \neg\varphi$$

なる文 φ を実際に作ることによって行なわれるが，この構成のための重要な要素が次の 6.4節で説明する**可証性述語**と 6.5節で証明する**対角化定理**である．

6.4 可証性述語

「理論 T における論理式 φ の証明」は 3.2 節で定義されたようにある条件を満たす論理式の有限列である．したがって，論理式のゲーデル数と有限列のコード化の技法を使って**証明のゲーデル数**を定義することができる．この詳細な定義は 9.2節で与えることにして，ここでは証明のゲーデル数が適切に定義されていると

して自然数上の次の 2 項関係 $\mathbf{Prov}_T(n,m)$ を考える．

$\mathbf{Prov}_T(n,m) \Leftrightarrow m$ は論理式 (φ とする) のゲーデル数であって，
n は「T における φ の証明」のゲーデル数である．(簡単に言えば「n が m を証明する」)

T が再帰的公理化可能ならばこの $\mathbf{Prov}_T$ は再帰的関係になる (このことは 9.2節の議論からもわかる)．すると再帰的関係の表現定理 (定理 5.6) によって，次の条件を満たす Q 上のΣ_1論理式 $\mathrm{Prov}_T(y,x)$ の存在が言える：任意の自然数 n,m について

(1) $\mathbf{Prov}_T(n,m)$ が成り立つときには $\mathrm{Q} \vdash \mathrm{Prov}_T(\overline{n},\overline{m})$,

(2) $\mathbf{Prov}_T(n,m)$ が成り立たないときには $\mathrm{Q} \vdash \neg\mathrm{Prov}_T(\overline{n},\overline{m})$.

定義．上に述べた論理式 $\mathrm{Prov}_T(y,x)$ を使って作った Q 上のΣ_1論理式

$$\exists y\, \mathrm{Prov}_T(y,x)$$

のことを T の**可証性述語 (provability predicate)** と呼び，これを

$$\mathrm{Pr}_T(x)$$

と表記する．

さて，可証性述語によって作られた文 $\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ すなわち $\exists y\, \mathrm{Prov}_T(y,\overline{\ulcorner\varphi\urcorner})$ の意味は「T における φ の証明がある，すなわち $T \vdash \varphi$」であり，実際

$$T \vdash \varphi \Leftrightarrow \mathfrak{N} \models \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

であることは，先程の (1)(2) と Q が $\mathfrak{N}$ をモデルとして持つことから明らかである．次の定理は，この右辺の「$\mathfrak{N} \models$」を「$T \vdash$ 」にした命題がどんな条件のもとで成り立つかを言っている．

定理 6.1　理論 T は Q の再帰的拡大であるとする．このとき T の任意の論理式 φ について次の (a)(b) が成り立つ．

(a) $T \vdash \varphi$ ならば $\mathrm{Q} \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$, したがって $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ である．

(b) T が ω無矛盾で $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ ならば $T \vdash \varphi$ である．

[証明] (a) Σ_1完全性定理 (定理 5.4) による．

(b) $T \nvdash \varphi$ と仮定すると $\mathbf{Prov}_T(n, \ulcorner\varphi\urcorner)$ はどんな自然数 n に対しても成り立たない．したがって先程の (2) によって，すべての n に対して $T \vdash \neg \mathrm{Prov}_T(\overline{n}, \overline{\ulcorner\varphi\urcorner})$ が成り立ち，$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ であるとすると T が ω矛盾することになる． □

注意．(1) 定理 6.1(a) の証明は，論理式 Pr_T が Σ_1 であることを使って Σ_1完全性定理によって行なった．しかしこの定理そして第一不完全性定理のためには，論理式 Prov_T が関係 $\mathbf{Prov}_T$ を表現してさえいれば (すなわち先程の (1)(2) が成り立てば) それで十分であり，Pr_T が Σ_1 である必要はない．

(2) 一方，第二不完全性定理のためには論理式 Pr_T の定義をやり直す必要がある．この詳細は 8.2節と 9.2節で説明する．

6.5 対角化定理

定理 6.2 (対角化定理 (diagonalization theorem)) $\varphi(x)$ は x 以外の自由変数を持たない任意の論理式であるとする．このとき

$$\mathrm{Q} \vdash \psi \leftrightarrow \varphi(\overline{\ulcorner\psi\urcorner})$$

なる文 ψ が存在する．

[証明] x 以外の自由変数を含まない論理式すべてを，そのゲーデル数の小さい順に並べて

$$A_0(x),\ A_1(x),\ A_2(x), \cdots$$

と呼ぶことにする．そして自然数上の関数 f を

$$f(n) = \ulcorner A_n(\overline{n}) \urcorner$$

(すなわち，n 番目の論理式に数項 $\overline{n}$ を代入して得られる文のゲーデル数) と定義する．ゲーデル数の性質からこの f は再帰的全域関数であり，再帰的全域関数の表現定理 (定理 5.8) によって,

$$(\dagger) \quad \mathrm{Q} \vdash \forall y (y = \overline{f(n)} \to \chi(\overline{n}, y)),$$

$$(\ddagger) \quad \mathrm{Q} \vdash \forall y (\neg(y = \overline{f(n)}) \to \neg\chi(\overline{n}, y)),$$

が任意の自然数 n について成り立つような論理式 $\chi(x,y)$ で，x, y 以外の自由変数を持たないものが存在する．ここで論理式 $\exists y(\chi(x,y)\land\varphi(y))$ を考える（この論理式は $\varphi(f(x))$ を意味している）．これは x 以外の自由変数を持たないので

$$A_k(x)\equiv\exists y(\chi(x,y)\land\varphi(y))$$

となるような自然数 k が存在するはずである．そこでこの k を使って，求める文 ψ を

$$\psi\equiv\exists y(\chi(\bar{k},y)\land\varphi(y))$$

と定義して（この文は $\varphi(f(\bar{k}))$ を意味している），次の (1)(2) を示す．

(1) $\mathrm{Q}\vdash\varphi(\overline{\ulcorner\psi\urcorner})\to\psi$.

(2) $\mathrm{Q}\vdash\neg\varphi(\overline{\ulcorner\psi\urcorner})\to\neg\psi$.

まず (†) と $f(k)=\ulcorner\psi\urcorner$ であること（なぜなら $\psi\equiv A_k(\bar{k})$ である）から

$$\mathrm{Q}\vdash\varphi(\overline{\ulcorner\psi\urcorner})\to(\chi(\bar{k},\overline{\ulcorner\psi\urcorner})\land\varphi(\overline{\ulcorner\psi\urcorner}))$$

が言えるので (1) が示される．一方 (2) の証明は

$$\mathrm{Q}\vdash\neg\varphi(\overline{\ulcorner\psi\urcorner})\to\forall y(\neg\chi(\bar{k},y)\lor\neg\varphi(y))$$

を示せばよいが，これは等号に関する推論による

$$\mathrm{Q}\vdash\neg\varphi(\overline{\ulcorner\psi\urcorner})\to\forall y(\neg(y=\overline{\ulcorner\psi\urcorner})\lor\neg\varphi(y))$$

と (‡) と $f(k)=\ulcorner\psi\urcorner$ から示される．□

注意．この対角化定理という名前は「対角線論法」による証明，すなわち

$$\begin{array}{llll}
A_0(\bar{0}) & A_0(\bar{1}) & A_0(\bar{2}) & \cdots\\
A_1(\bar{0}) & A_1(\bar{1}) & A_1(\bar{2}) & \cdots\\
A_2(\bar{0}) & A_2(\bar{1}) & A_2(\bar{2}) & \cdots\\
\vdots & \vdots & \vdots & \ddots
\end{array}$$

の対角線を考えていることに由来している．なお $\mathrm{Q}\vdash\psi\leftrightarrow\varphi(\overline{\ulcorner\psi\urcorner})$ を見ると ψ は $\varphi(x)$ の「不動点」に見えるので，この定理は不動点定理 **(fixed point theorem)** と呼ばれることもある．

6.6 ゲーデルの第一不完全性定理

定義. 理論 T の文 φ が

$$T \vdash \varphi \leftrightarrow \neg \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$$

を満たすとき，φ は T のゲーデル文であると言う．

ゲーデル文は T 上の Π_1文であり,「自分自身は証明できない」という意味の文になる (これは「私は嘘をついている」というパラドックスと状況が似ている)．

さて，可証性述語 $\mathrm{Pr}_T(x)$ が存在し (すなわち T が再帰的公理化可能であり)，T が Q の拡大であるならば，対角化定理 (定理 6.2) によってゲーデル文の存在が示される．するとこれを用いて第一不完全性定理を証明することができる．

定理 6.3 (ゲーデルの第一不完全性定理)
理論 T が Q の再帰的拡大ならば T のゲーデル文 φ に対して次が成り立つ：

(a) T が無矛盾ならば $T \nvdash \varphi$ である．

(b) T が ω無矛盾ならば $T \nvdash \neg\varphi$ である．

したがって，T が ω無矛盾ならば T は不完全である．

[証明] (a) 後の都合 (第二不完全性定理の証明) のために，やや冗長な証明をステップごとに番号をつけて行なう．

(1) $T \vdash \varphi$ を仮定すると定理 6.1(a) によって $T \vdash \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$ である．

(2) $T \vdash \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$ ならばゲーデル文の定義を用いて $T \vdash \neg\varphi$ になる．

(3) 以上の (1), (2) により，$T \vdash \varphi$ を仮定すると $T \vdash \neg\varphi$ である．

(4) したがって，$T \vdash \varphi$ を仮定すると $T \vdash \varphi$ かつ $T \vdash \neg\varphi$, すなわち T は矛盾する．

(5) したがって，T が無矛盾ならば $T \nvdash \varphi$ である．

(b) $T \vdash \neg\varphi$ を仮定するとゲーデル文の定義を用いて $T \vdash \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$ となる．すると定理 6.1(b) (ここで「ω無矛盾」の仮定を使用する) によって $T \vdash \varphi$ になるが，これは (a) に反する．したがって $T \nvdash \neg\varphi$ である． □

第一不完全性定理からただちに以下の 2 つの定理が導かれる．

定理 6.4　Q も PA も不完全である．

[証明]　Q も PA も $\mathfrak{N}$ をモデルとして持つので ω無矛盾であり，またどちらも Q の再帰的拡大である．□

定理 6.5 (無矛盾かつ ω矛盾する理論の存在定理)　理論 T は Q の無矛盾な再帰的拡大とする．いま T のゲーデル文を φ とし，T に公理 $\neg\varphi$ を加えた理論を T' とすると，T' は無矛盾だが ω矛盾する理論になる．

[証明]　T' が無矛盾であることを示すには $T \nvdash \varphi$ を示せばよいが (演繹定理 (定理 3.2) による)，これは第一不完全性定理 (a) である．一方，ゲーデル文の定義や $T \nvdash \varphi$ であることなどから

$$T' \vdash \exists y \mathrm{Prov}_T(y, \overline{\ulcorner\varphi\urcorner}),$$

すべての自然数 n について $T' \vdash \neg\mathrm{Prov}_T(\overline{n}, \overline{\ulcorner\varphi\urcorner})$,

となって，T' が ω矛盾することが示される．□

注意．(1) T が Q の無矛盾な再帰的拡大で φ が Tのゲーデル文ならば，第一不完全性定理 (a) およびゲーデル文の定義などによって，$\neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ は「正しいけれども T では証明できない Π_1文」になることがわかる．さらに，T が $\mathfrak{N}$ をモデルとして持つ場合はゲーデル文の定義から

$$\mathfrak{N} \models \varphi \leftrightarrow \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

となるので，ゲーデル文 φ も「正しいけれども T では証明できない Π_1文」になることがわかる．

(2) 第一不完全性定理を可証性述語や対角化定理を使わずに次の方針で証明することもできる．まず T が Q の再帰的拡大 (RE 拡大でもよい) で ω無矛盾ならば，自然数上の 1 項関係 $A(n)$ に関する次の 2 条件が同値になることが補題 4.14(7) や再帰的関係の表現定理 (定理 5.6) などから示される：

- $A(n)$ は RE.

- x 以外の自由変数を含まない論理式 $\varphi(x)$ が存在して，任意の自然数 n に対して

$$A(n) \text{ が成り立つ} \Leftrightarrow T \vdash \varphi(\overline{n}).$$

ここで，RE であるが再帰的ではない関係を $A(n)$ として (定理 4.19), この $A(n)$ に対して上で得られる論理式を $\varphi(x)$ とすると，$\neg A(n)$ が RE でないこと (定理 4.18) などから

$$T \nvdash \varphi(\overline{n}), \quad T \nvdash \neg\varphi(\overline{n})$$

なる n が存在することが導かれる．

第 7 講　第一不完全性定理の拡張

7.1　ロッサーの不完全性定理

ゲーデルの第一不完全性定理は

(a) $T \vdash \varphi$ ならば $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$,

(b) $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ ならば $T \vdash \varphi$,

(c) $T \vdash \varphi \leftrightarrow \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$,

なる文 φ を使って示されたが，(b) を示すために T が ω無矛盾であるという条件が必要であった．これに対してロッサー (J.B. Rosser) は $\mathrm{Pr}_T(x)$ とは少し異なる論理式 $\mathrm{Pr}^*_T(x)$ (これをロッサーの可証性述語と呼ぶ) を定義して，これが任意の φ に対して

(d) $T \vdash \varphi$ ならば $T \vdash \mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$,

(e) $T \vdash \neg\varphi$ ならば $T \vdash \neg\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$,

を満たすことを示した．この際 T が ω無矛盾である必要はない．そして

(f) $T \vdash \varphi \leftrightarrow \neg\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$,

なる文 φ (このような φ のことを T のロッサー文と呼ぶ) をとることによって次が言える．

定理 7.1　理論 T が無矛盾で T の論理式 $\mathrm{Pr}^*_T(x)$ が上の (d), (e) を満たし φ が T のロッサー文ならば，$T \nvdash \varphi$ かつ $T \nvdash \neg\varphi$, すなわち T は不完全である．

[証明]　$T \vdash \varphi$ と仮定すると，(d), (f) からそれぞれ $T \vdash \mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$, $T \vdash \neg\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$ で T が矛盾してしまう．$T \vdash \neg\varphi$ と仮定すると，同様に (e) と (f) から T が矛盾することが導かれる．□

それでは実際にロッサーの可証性述語 $\mathrm{Pr}^*_T(x)$ をどのように定義するか説明しよう．理論 T は Q の再帰的拡大であるとする．6.4節で定義した $\mathrm{Prov}_T(y, x)$ は自然数上の再帰的関係 $\mathbf{Prov}_T(n, m)$ を Q で表現した Σ_1論理式であった．同様

に，自然数上の関係

$$\mathbf{Dispr}_T(n,m) \;\Leftrightarrow\; m \text{ は論理式 } (\varphi \text{ とする}) \text{ のゲーデル数であって}, n \text{ は「} T \text{ における } \neg\varphi \text{ の証明」のゲーデル数である}$$

は再帰的であり，これを Q で表現する Π_1 論理式 $\mathrm{Dispr}_T(y,x)$ が存在する (disprove: 反証する)．そして

$$\mathrm{Pr}^*_T(x) \equiv \exists y(\mathrm{Prov}_T(y,x) \land \forall z{<}y\, \neg\mathrm{Dispr}_T(z,x))$$

とする (これは Q 上の Σ_1 論理式となる)．文 $\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$ の意味は「φ の証明 y があって，y よりゲーデル数が小さなものはどれも $\neg\varphi$ の証明ではない」ということであり，$\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ よりも少し強いことを主張していることがわかる．

定理 7.2 (ロッサーの可証性述語の性質) 理論 T が Q の再帰的拡大ならば，任意の論理式 φ に対して次の (1), (2) が成り立つ．

(1) $T \vdash \varphi$ ならば $T \vdash \mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$.

(2) $T \vdash \neg\varphi$ ならば $T \vdash \neg\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$.

[証明] もし T が矛盾するならば明らかにこれらは成り立つ．そこで T は無矛盾であるとする．$T \vdash \varphi$ であって T が無矛盾ならば $\mathrm{Pr}^*_T(\overline{\ulcorner\varphi\urcorner})$ は Q 上の正しい Σ_1 文になるので，Σ_1完全性定理 (定理 5.4) によって (1) が示される．一方 $T \vdash \neg\varphi$ のときは，T における $\neg\varphi$ の証明があるのでその証明のゲーデル数を n とする．すると $\mathbf{Dispr}_T(n, \ulcorner\varphi\urcorner)$ が成り立ち，さらに T の無矛盾性から $\mathbf{Prov}_T(i, \ulcorner\varphi\urcorner)$ はどんな i についても成り立たない．したがって

$$\mathrm{Q} \vdash \mathrm{Dispr}_T(\overline{n}, \overline{\ulcorner\varphi\urcorner}),$$

$$n \text{ 以下のすべての } i \text{ に対して } \mathrm{Q} \vdash \neg\mathrm{Prov}_T(\overline{i}, \overline{\ulcorner\varphi\urcorner})$$

が成り立ち，定理 5.3(d) の証明と同様にして

$$\mathrm{Q} \vdash \forall y(\neg\mathrm{Prov}_T(y, \overline{\ulcorner\varphi\urcorner}) \lor \exists z{<}y\mathrm{Dispr}_T(z, \overline{\ulcorner\varphi\urcorner}))$$

となって (2) が示される．□

さて，T が Q の拡大ならば対角化定理 (定理 6.2) によってロッサー文の存在は保証されるので，以上の定理 7.1, 7.2から次が言える．

定理 7.3 (ゲーデル・ロッサーの不完全性定理) Q の無矛盾な再帰的拡大は不完全である．

7.2　クレイグの手法

2 つの理論 T と T' が，任意の論理式 φ に対して

$$T \vdash \varphi \;\Leftrightarrow\; T' \vdash \varphi$$

であるとき，T と T' は同等であると言う．さて次の定理は「クレイグ (W. Craig) の手法」として知られているものである．

定理 7.4　RE 公理化可能などんな理論 T に対しても，それと同等な再帰的公理化可能な理論 T' が存在する．

[証明]　T を RE 公理化可能な理論とする．すると 4.4 節の補題 4.14 によって

$$\mathbf{Axiom}_T(n) \text{ が成り立つ} \;\Leftrightarrow\; \text{ある } m \text{ が存在して } \mathbf{B}(n,m) \text{ が成り立つ}$$

となるような再帰的 2 項関係 $\mathbf{B}$ が存在するので，この $\mathbf{B}$ を使って理論 T' を次のように定義する：T' の固有の公理の集合 $\mathrm{Axiom}_{T'}$ を

$$\mathrm{Axiom}_{T'} = \{\overbrace{\varphi \wedge \varphi \wedge \cdots \wedge \varphi}^{m+1\text{ 個}} \mid \varphi \text{ は } T \text{ の固有の公理で，} m \text{ は } \mathbf{B}(\ulcorner\varphi\urcorner, m) \text{ が成り立つ最小の自然数}\}$$

とする．すると

$$\vdash \varphi \leftrightarrow (\varphi \wedge \varphi \wedge \cdots \wedge \varphi)$$

であることから明らかに T と T' は同等である．さらに，任意に与えられた ψ が T' の固有の公理か否かの判定は，ψ を

$$\overbrace{\varphi \wedge \varphi \wedge \cdots \wedge \varphi}^{m+1}$$

という形に分解して $\mathbf{B}(\ulcorner\varphi\urcorner, m)$ が成り立つか否かを判定することによって行なえるので，$\mathbf{Axiom}_{T'}$ は再帰的である．□

この定理と先程のゲーデル・ロッサーの不完全性定理 (定理 7.3) によって次が得られる．

定理 7.5 (クレイグの手法による第一不完全性定理の拡張) Q の無矛盾な RE 拡大は不完全である.

7.3 決定不能性に関するいくつかの結果

第一不完全性定理の証明の手法を使うと，算術や述語論理の重要な性質を示すことができる．ここではそのような結果をいくつか紹介しよう．

補題 7.6 理論 T は Q の無矛盾な拡大であるとする．このとき次の条件を満たす 1 変数論理式 $A(x)$ は存在しない：任意の文 φ について，

$T \vdash \varphi$ ならば $T \vdash A(\overline{\ulcorner\varphi\urcorner})$,

$T \nvdash \varphi$ ならば $T \vdash \neg A(\overline{\ulcorner\varphi\urcorner})$.

[証明] このような $A(x)$ があると仮定すると対角化定理 (定理 6.2) によって

(1) $T \vdash \psi \leftrightarrow \neg A(\overline{\ulcorner\psi\urcorner})$

なる文 ψ を得ることができる．この ψ に上の条件を適用すると

(2) $T \vdash \psi$ ならば $T \vdash A(\overline{\ulcorner\psi\urcorner})$,

(3) $T \nvdash \psi$ ならば $T \vdash \neg A(\overline{\ulcorner\psi\urcorner})$,

となるが，無矛盾な T は (1)(2)(3) を同時に成り立たせることはできない．□

これからこの補題を使って算術や述語論理の性質を証明していくが，その前にひとつ定義をしておこう．Q に $\mathfrak{N} \models \varphi$ なるすべての文 φ を公理として加えた理論を TA(True Arithmetic) と呼ぶ．すると任意の文 ψ に対して

$\mathrm{TA} \vdash \psi \iff \mathfrak{N} \models \psi$

であり，TA は ω無矛盾かつ完全である．(したがって第一不完全性定理により TA は再帰的公理化可能ではないことがわかる．) 上の補題 7.6は T が再帰的公理化可能でないときにも適用可能であり，T として特に TA をとることができる点に注意されたい．

定理 7.7 (タルスキの真偽定義不能性定理) 次を条件 (†) を満たす 1 変数論理式 $A(x)$ は存在しない：

$$(\dagger)\ \text{任意の文}\ \varphi\ \text{について}\ \mathfrak{N} \models \varphi \leftrightarrow A(\ulcorner\varphi\urcorner).$$

[証明]　このような $A(x)$ は，$T = \mathrm{TA}$ としたときの補題 7.6の条件を満たす論理式になる．□

上の (†) を満たす論理式 $A(x)$ は (もしあったとしたら)「任意の文の真偽を記述した論理式」もしくは「任意の文の真偽を定義する論理式」であると言える．したがってこの定理は「1 階算術の文の自然数上での真偽は 1 階算術の論理式では定義できない」ということを示している．

定理 7.8 (Q の本質的決定不能性定理) Q のどんな無矛盾な拡大も決定不能である．すなわち，理論 T が Q の拡大で無矛盾であるとき，自然数上の 1 項関係 $\mathbf{Pr}_T$ を

$$\mathbf{Pr}_T(n)\ \Leftrightarrow\ n\ \text{は}\ T \vdash \varphi\ \text{なる文}\ \varphi\ \text{のゲーデル数}$$

と定義すると，$\mathbf{Pr}_T$ は再帰的関係ではない．

[証明]　$\mathbf{Pr}_T$ が再帰的であると仮定すると，再帰的関係の表現定理 (定理 5.6) によって補題 7.6の条件を満たす論理式の存在が言えてしまう．□

この定理によって「T が Q の無矛盾な RE 拡大ならば，$\mathbf{Pr}_T$ は RE だが再帰的ではない」ということが言える．

定理 7.9 ($\mathfrak{N}$ の決定不能性定理) 自然数上の 1 項関係 **True** を

$$\mathbf{True}(n)\ \Leftrightarrow\ n\ \text{は}\ \mathfrak{N} \models \varphi\ \text{なる文}\ \varphi\ \text{のゲーデル数}$$

とすると，**True** は再帰的関係ではない．したがって，任意に与えられた文の自然数上での真偽を判定するアルゴリズムはない．

[証明]　直前の定理 7.8の T として TA をとればよい．□

定理 7.10 (述語論理の決定不能性定理) 「与えられた文が述語論理で証明可能か否か？」という問題は決定不能である．

[証明] Q の固有の公理 **A1〜A7** を ∧ でつないでひとつにまとめた文を Q と名付ける．すると演繹定理 (定理 3.2) により，Q の任意の文 φ に対して

$$\mathrm{Q} \vdash \varphi \iff \vdash Q \to \varphi$$

である．したがって，もしも述語論理が決定可能ならば Q も決定可能になってしまうが，これは先程の定理 7.8に反する．□

注意. 本書での「述語論理」は等号に関する公理 (30 ページの P5, P6) を含んでいるが，上の証明と同様にして「等号に関する公理を持たない述語論理」の決定不能性も導かれる．なぜなら，次の 6 つの文

$$\forall x(x = x), \quad \forall x\,\forall y\,(x = y \to y = x), \quad \forall x\,\forall y\,\forall z\,(x = y \land y = z \to x = z),$$

$$\forall x\,\forall y\,(x = y \to \mathrm{S}(x) = \mathrm{S}(y)), \quad \forall x\,\forall y\,\forall u\,\forall v\,(x = y \land u = v \to x + u = y + v),$$

$$\forall x\,\forall y\,\forall u\,\forall v\,(x = y \land u = v \to x{\cdot}u = y{\cdot}v),$$

をすべて ∧ でつないだ文を E とすると，Q の任意の文 φ に対して

$$\mathrm{Q} \vdash \varphi \iff \vdash' (Q \land E) \to \varphi$$

(ただし $\vdash'$ は等号に関する公理を使わずに証明できることを表す) が成り立つからである．

第8講　第二不完全性定理

8.1　第二不完全性定理の意義

第二不完全性定理の内容と意義について簡単に説明しよう．

理論 T が無矛盾 (consistent) であるとは $T \nvdash \bot$ ということであるが (6.3節参照)，これを意味する T の文 $\mathrm{Con}(T)$ を次のように定める．

定義．$\mathrm{Con}(T) \equiv \neg\mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner})$. (ただし可証性述語 Pr_T に関して注意が必要であり，次節および 9.2節でそれを詳しく述べる．)

さて次の定理がゲーデルの第二不完全性定理である：

> 理論 T が PA の RE 拡大で無矛盾ならば，$T \nvdash \mathrm{Con}(T)$ である．すなわち無矛盾な T は自分自身の無矛盾性を証明できない．

したがって，T が無矛盾ならば $\mathrm{Con}(T)$ は正しいけれども T では証明できない Π_1文になる．

ところで「正しいけれども T では証明できないΠ_1文」といえば，ゲーデル文 (またはゲーデル文 φ を用いた文 $\neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$) がそうであった．しかしゲーデル文は対角化定理によって人工的に作られた論理式，という感があるのに対して，$\mathrm{Con}(T)$ は理論の無矛盾性を表現した具体的な意味を持つ論理式である点が第二不完全性定理の重要なところである．「数学の理論の無矛盾性をできるだけ弱い道具 (有限の立場) で証明せよ」という当時の大問題 — ヒルベルトのプログラム (の一部分) — に対して，ゲーデルは一つの普遍的な否定解を与えたのである．(ヒルベルトのプログラムについては補講を参照されたい．)

しかし第二不完全性定理の意義は決して否定的なものではない．この定理が明らかにしたことは「無矛盾性」が理論の強さを分類する指標になるということである．つまり，二つの理論の強さが異なることを証明する手段として「『片方が片方の無矛盾性を証明する』ことを示す」という方法が確立されたのである．

またゲーデルによる第二不完全性定理の証明方法も重要である．第二不完全性定理は第一不完全性定理の証明を T の中で形式化して行なうことによって導かれるが，この手法 — メタな証明を形式化して行なうこと — はこの分野の研究における最も重要な証明手法の一つとなったのである．

なお第一不完全性定理の証明中 (たとえば定理 5.1の証明) で数学的帰納法を用いているが，このメタな証明を T の中で形式化して行なうために T が帰納法の公理を持っている必要がある．この理由によって第二不完全性定理には「T が PA の RE 拡大ならば」という前提条件が必要になっている．(第一不完全性定理の前提条件は「T が Q の RE 拡大ならば」であった．)

8.2 可導性条件と第二不完全性定理

第二不完全性定理を証明するためには可証性述語の性質を詳しく調べる必要がある．以下の **D1〜D3** は，この定理の見通しの良い証明を与えるためにレーブ (M.H. Löb) が与えた**可導性条件** (**Derivability Conditions**) と呼ばれるものである．

D1: $T \vdash \varphi$ ならば $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$.

D2: $T \vdash (\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \wedge \mathrm{Pr}_T(\overline{\ulcorner\varphi \to \psi\urcorner})) \to \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner})$.

D3: $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})\urcorner})$.

(ただし φ, ψ は T の任意の論理式．) この節ではこれらを用いて第二不完全性定理を証明する．

ところで，第一不完全性定理を示すための可証性述語 $\mathrm{Pr}_T(x) \equiv \exists y \mathrm{Prov}_T(y, x)$ は，Prov_T が関係 $\mathbf{Prov}_T$ を表現した Σ_1論理式 (あるいは Σ_1 でなくてもよい) であれば何でもよかった．しかしこの条件では一般に $T \nvdash \neg\mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner})$ は成り立たない：

> たとえばロッサーの可証性述語を考えると，定理 7.2(2) により
> $T \vdash \neg\mathrm{Pr}^*_T(\overline{\ulcorner\bot\urcorner})$ となり，この論理式を「T の無矛盾性を表す文」だと
> 思うと「T の無矛盾性が T で証明された」ということになる．

このため第二不完全性定理のための可証性述語 $\mathrm{Pr}_T(x)$ は適切に定義される必要があるのだが，その定義を示すには多くの準備が必要となる．そこで，とりあえずこの節では PA 上の Σ_1論理式 $\mathrm{Pr}_T(x)$ が存在して，それが可証性述語としての当然の条件

$$T \vdash \varphi \;\Leftrightarrow\; \mathfrak{N} \models \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

を満たし，さらに可導性条件 (次の定理 8.1) が成り立つものとして先へ進む．論理式 $\mathrm{Pr}_T(x)$ の具体的な定義と可導性条件 **D2**, **D3** の詳細な証明は第 9 講で与えられる．

定理 8.1 (可導性条件) 理論 T が PA の RE 拡大ならば可導性条件 **D1**〜**D3** が成り立つ．

[証明] **D1** は定理 6.1(a) と同じ (Q を PA に変える) であり，Σ_1完全性定理 (定理 5.4) により明らか．**D2** は,「証明 P のゲーデル数 x と証明 Q のゲーデル数 y と論理式 ψ のゲーデル数 k をもらって，P と Q と ψ を順に並べた証明のゲーデル数を返す」ような関数 $g(x,y,k)$ が PA の項として書けて，

$$T \vdash \forall x \forall y((\mathrm{Prov}_T(x, \overline{\ulcorner\varphi\urcorner}) \land \mathrm{Prov}_T(y, \overline{\ulcorner\varphi \to \psi\urcorner})) \to \mathrm{Prov}_T(g(x,y,\overline{\ulcorner\psi\urcorner}), \overline{\ulcorner\psi\urcorner}))$$

となることを示せば，述語論理の推論によって **D2** の論理式も T で証明できることがわかる (定理 9.3)．**D3** の論理式は **D1** を T の論理式で表した形をしている．**D1** の証明には Σ_1完全性定理が使われていたのだが，ここで次の形式化された Σ_1完全性定理 (定理 9.4) が成り立つ：

$$T\text{上の任意の } \Sigma_1\text{文 } \sigma \text{ に対して } T \vdash \sigma \to \mathrm{Pr}_T(\overline{\ulcorner\sigma\urcorner}).$$

$\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ は T 上の Σ_1文なので，この σ を $\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ にすることによって **D3** を得る．□

それでは，ひとつ補題を示してから第二不完全性定理の証明を行なおう．

補題 8.2　可導性条件 **D1**, **D2** が成り立つならば，次の (1), (2) が成り立つ．

(1) $T \vdash \varphi \to \psi$ ならば $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner})$.

(2) $T \vdash (\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \wedge \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner})) \to \mathrm{Pr}_T(\overline{\ulcorner\varphi \wedge \psi\urcorner})$.

[証明] (1) $T \vdash \varphi \to \psi$ を仮定すると **D1** より $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi \to \psi\urcorner})$ となり，**D2** と命題論理の推論によって $T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner})$ を得る．

(2) $\varphi \to (\psi \to (\varphi \wedge \psi))$ は命題論理で証明できるので，(1) によって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\psi \to (\varphi \wedge \psi)\urcorner})$$

となる．一方 **D2** より

$$T \vdash (\mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner}) \wedge \mathrm{Pr}_T(\overline{\ulcorner\psi \to (\varphi \wedge \psi)\urcorner})) \to \mathrm{Pr}_T(\overline{\ulcorner\varphi \wedge \psi\urcorner})$$

であるので，これらから (2) は導かれる．□

定理 8.3 (ゲーデルの第二不完全性定理) 理論 T が PA の RE 拡大で無矛盾ならば $T \nvdash \mathrm{Con}(T)$ である．

[証明] φ を T のゲーデル文とする (ゲーデル文の定義と存在については 6.6節参照)．まず第一不完全性定理 (定理 6.3) の (a) を意味する論理式

$$\mathrm{Con}(T) \to \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

が T で証明できることを可導性条件 (定理 8.1, 補題 8.2) を使って示す．(以下の証明を第一不完全性定理 (a) の証明と見比べてみよ.)

(1) 可導性条件 **D3** より

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})\urcorner}).$$

(2) φ はゲーデル文なので

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \neg\varphi$$

であり，補題 8.2の (1) により

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\neg\varphi\urcorner}).$$

(3) 以下の (1), (2) により

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\neg\varphi\urcorner}).$$

(4) したがって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to (\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \wedge \mathrm{Pr}_T(\overline{\ulcorner\neg\varphi\urcorner}))$$

であるが，一方 $(\varphi \land \neg\varphi) \to \bot$ は命題論理で証明できるので，これらと補題 8.2の (1)(2) によって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner}).$$

(5) したがって，$\mathrm{Con}(T)$ の定義と合わせて

$$T \vdash \mathrm{Con}(T) \to \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}).$$

以上が第一不完全性定理 (a) の証明を形式化して T の中で行なったものである．ところで第一不完全性定理 (a):

$$T \text{ が無矛盾ならば } T \nvdash \varphi$$

そのものも，可導性条件 **D1** を用いて 6.6節での証明とまったく同じ方法で示すことができる．したがって，このことと T は無矛盾であるという仮定とゲーデル文の定義から

$$T \nvdash \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

となり，上の (5) と組み合わせて

$$T \nvdash \mathrm{Con}(T)$$

となる．□

8.3　可証性述語のいくつかの性質

可導性条件を用いると第二不完全性定理のほかにも $\mathrm{Pr}_T(x)$ のさまざまな性質を示す事ができる．ここではそのような結果をいくつか紹介しよう．

定理 8.4　理論 T が PA の RE 拡大で無矛盾ならば，どんな論理式 φ に対しても $T \nvdash \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ である．(第二不完全性定理は特に φ が $\bot$ の場合であった．)

[証明]　$T \vdash \bot \to \varphi$ であるので，可導性条件 (定理 8.1, 補題 8.2) によって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}).$$

となる．したがって，もしも $T \vdash \neg\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ ならば $T \vdash \neg\mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner})$ となってしまい，第二不完全性定理 (定理 8.3) に反する．□

論理式 φ, ψ について，

$$T \vdash \varphi \leftrightarrow \psi$$

であるとき, T上で φ と ψ は同等であると言う．

定理 8.5 理論 T が PA の RE 拡大ならば，T のゲーデル文は T 上で $\mathrm{Con}(T)$ と同等である．

[証明] φ を T のゲーデル文とする．

$$T \vdash \neg \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner}) \to \mathrm{Con}(T)$$

が定理 8.4の証明から言えるので，ゲーデル文の定義と合わせると

$$T \vdash \varphi \to \mathrm{Con}(T)$$

である．一方，第二不完全性定理 (定理 8.3) の証明中の (5) とゲーデル文の定義によって

$$T \vdash \mathrm{Con}(T) \to \varphi$$

である．□

定理 8.6 (レーブの定理) 理論 T が PA の RE 拡大ならば，任意の文 φ に対して

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner}) \to \varphi \iff T \vdash \varphi$$

である．

[証明] 左向き ($\Leftarrow$) は明らか．右向き ($\Rightarrow$) は

$$(1)\ T \vdash \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner}) \to \varphi$$

を仮定して，$T \vdash \varphi$ であることを可導性条件 (定理 8.1, 補題 8.2) を使って次のように導く．対角化定理 (定理 6.2) によって

$$(2)\ T \vdash \psi \leftrightarrow (\mathrm{Pr}_T(\overline{\ulcorner \psi \urcorner}) \to \varphi)$$

を満たす文 ψ を得ることができる．すると，この片向き $(\psi \to (\mathrm{Pr}_T(\overline{\ulcorner \psi \urcorner}) \to \varphi))$ と補題 8.2(1) と可導性条件 **D2** によって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner \psi \urcorner}) \to (\mathrm{Pr}_T(\overline{\ulcorner \mathrm{Pr}_T(\overline{\ulcorner \psi \urcorner}) \urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner}))$$

となる．するとこれから，可導性条件 **D3** と命題論理の推論によって

$$T \vdash \mathrm{Pr}_T(\overline{\ulcorner \psi \urcorner}) \to \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$$

となるので，(1) によって

$$(3)\ T \vdash \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner}) \to \varphi$$

を得る．すると (2) と (3) から

$$T \vdash \psi$$

となって，これに可導性条件 **D1** を適用して，(3) とあわせると

$$T \vdash \varphi$$

が導かれる．□

8.4　可証性述語と様相論理

第二不完全性定理や前節での結果の証明には可導性条件は必要であったが論理式 $\mathrm{Pr}_T(x)$ の定義は直接必要はなかった．すなわち $\mathrm{Pr}_T(x)$ の「実体」ではなく「働き」だけに着目した議論を行なったのである．働きだけに着目するということは $\mathrm{Pr}_T(x)$ を様相演算子 □ と見なして様相論理を考察することにほかならないが，ここではそのような研究の出発点となったソロベイ (**R.M. Solovay**) の結果を紹介しよう．なお様相論理に関する基本的な事項については，たとえばパート A の参考文献 [1] を参照されたい．

可証性述語 Pr_T を様相演算子 □ と見なすと，可導性条件は

D1: $\dfrac{A}{\Box A}$

D2: $(\Box A \land \Box(A \to B)) \to \Box B$

D3: $\Box A \to \Box\Box A$

という様相論理の推論規則 (**D1**) ならびに公理 (**D2**, **D3**) と読むことができる．命題論理にこれらの規則，公理を加えた様相命題論理の体系は K4 という名前で知られているが，K4 にさらに推論規則

$$\frac{\Box A \to A}{A}$$

(これはレーブの定理 (定理 8.6) に対応している) を加えた体系を GL_1 と呼び，K4 に公理

$$\Box(\Box A \to A) \to \Box A$$

(これはレーブの定理を形式化した論理式に対応している) を加えた体系を GL_2 と呼ぶことにする．すると，じつはこの 2 つの体系の証明能力は同じになる．そこで改めてこれらの体系をともに GL (ゲーデル，レーブの頭文字) と呼ぶことにする．

GL の論理式は原子命題と $\neg$, $\rightarrow$, $\Box$ から構成されるが，原子命題に算術の理論 T の文を割り当て，$\Box\varphi$ を $\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ に変えることによって，GL の論理式を T の文に翻訳することができる．GL の論理式 A をこのように翻訳して得られる T の文のことを A^* と表わすことにする．この翻訳は GL の各原子命題に T のどんな文を割り当てるかを定めることによって決定される．

例: A が $p \rightarrow \Box(q \rightarrow \Box p)$ で，原子命題 p と q にそれぞれ T の文 $0=0$ と $\forall x\forall y(x=y)$ を割り当てるならば

$$A^* \equiv 0=0 \rightarrow \mathrm{Pr}_T(\overline{\ulcorner\forall x\forall y(x=y) \rightarrow \mathrm{Pr}_T(\overline{\ulcorner 0=0\urcorner})\urcorner})$$

である．

1976 年にソロベイは「様相命題論理の体系 GL は算術の可証性述語の性質にちょうど一致している」という次の定理を証明した．

定理 8.7 (GL に関するソロベイの完全性定理) T が PA の ω無矛盾な RE 拡大ならば，GL の任意の論理式 A について次の (1), (2) は同値．

(1) $\mathrm{GL} \vdash A$.

(2) どんな翻訳 $*$ に対しても $T \vdash A^*$.

[証明の方針] (1)⇒(2) は可導性条件とレーブの定理により明らか．(2)⇒(1) は対偶を証明する．これは

$$\mathrm{GL} \nvdash A \;\Rightarrow\; \text{GL のクリプキモデル } M \text{ が存在して } M \not\models A$$

(GL のクリプキモデルに対する完全性定理) を用いて，この M の情報を使って $T \nvdash A^*$ となるような翻訳 $*$ を定義することによって示される．□

さらにソロベイは，次の 2 条件が同値になるような様相論理の体系 GLS も与えた．

- $\mathrm{GLS} \vdash A$.
- どんな翻訳 $*$ に対しても $\mathfrak{N} \models A^*$.

これらの結果を出発点として可証性述語と様相論理とを関連させる研究が盛んに行なわれている．詳細についてはこのパートの参考文献 [1][2] を参照されたい．

第 9 講　可証性述語の詳細

9.1　β関数定理の形式化

第 8 講では可証性述語 $\mathrm{Pr}_T(x)$ の直接の定義は与えずにそれが持つ性質 (可導性条件) だけを使った議論を行なったが，この講では $\mathrm{Pr}_T(x)$ の定義を与え可導性条件の証明などの詳細な議論を行なう．そしてその準備として，この 9.1節では「パート A の 4.5節での議論を PA の中で形式化して行なうこと」について説明する．

定理 9.1 β, γ, δ をそれぞれ 4.5節で導入した関数とする．すると関係 $\beta(x,y,z)=v$, $\gamma(x)=v$, $\delta(x)=v$ をそれぞれ意味する PA 上の Δ_1論理式 $B(x,y,z,v)$, $C(x,v)$, $D(x,v)$ があって，文 $\forall x \forall y \forall z\, \exists! v\, B(x,y,z,v)$, $\forall x\, \exists! v\, C(x,v)$, $\forall x\, \exists! v\, D(x,v)$ がそれぞれ PA で証明できる．

[証明]　$\mathrm{rm}(x,y)=z$ を意味する Δ_1論理式としては

$$\exists a \leqq x (y{\cdot}a + z = x) \land z < y$$

がある．(ただし $\exists a \leqq x(\cdots) \equiv \exists a < \mathrm{S}(x)(\cdots)$ である．なお $z<y$ が PA 上で Δ_1 であることは簡単に示される．) また，$\bigvee_{i=0}^{x} f(i) = y$ を意味する Δ_1論理式としては

$$\forall i \leqq x (f(i)|y) \ \land\ y > 0\ \land\ \forall z{<}y\, \neg(\forall i \leqq x (f(i)|z) \land z > 0)$$

(ただし $f(i)|y$ は $\mathrm{rm}(y, f(i)) = 0$ に相当する論理式) がある．そこでこれらを使って求める $B(x,y,z,v)$, $C(x,v)$, $D(x,v)$ を作ることができる．□

この定理と 3.4 節の系 3.11とその直後の議論によって，以後必要に応じて PA には関数記号 β, γ, δ があると仮定する．さらに「z は $\{y, f(0), \cdots, f(x)\}$ の中の最大値である」を意味する Δ_1論理式としては

$$(y = z \lor \exists i \leqq x (f(i) = z)) \land y \leqq z \land \forall i \leqq x (f(i) \leqq z)$$

があり，$f(x)$ が PA の項のときに $\{y, f(0), \cdots, f(x)\}$ の中の最大値の一意存在性

があり，$f(x)$ が PA の項のときに $\{y, f(0), \cdots, f(x)\}$ の中の最大値の一意存在性を PA で証明できるので，「$\{y, f(0), \cdots, f(x)\}$ の中の最大値」を意味する PA の項

$$\max_{i=0}^{x}(y; f(i))$$

があることも仮定する．

さて，4.5節で β関数定理の証明に至る過程で使われた自然数の性質 (たとえば「ある条件を満たす自然数が存在するならば，その条件を満たす最小の自然数が存在する」など) は，すべて数学的帰納法によって導くことができる．したがって 4.5節での議論をすべて PA の内部で行なうことができて，次の定理が得られる．

定理 9.2 (形式化された β関数定理) $f(x, n, \overrightarrow{y})$ を PA の項とする．すると

$$\mathrm{PA} \vdash \forall \overrightarrow{y}\ \forall n\ \exists a < \gamma(m)\ \forall i \leqq n\ (\beta(a, \delta(m), i) = f(i, n, \overrightarrow{y})),$$

$$\text{ただし } m \equiv \max_{i=0}^{n}(n; f(i, n, \overrightarrow{y}))$$

である．

上の論理式は「$f(x, n, \overrightarrow{y})$ の x 以外の変数の値を任意に固定して 1 変数関数と見たときに β関数定理 (定理 4.24) が成り立つ」と読むことができる．なお，この節の議論の詳細については参考文献 [1] も参照されたい．

9.2　可証性述語の定義

ここでは前節での議論を踏まえて，第二不完全性定理のための可証性述語 $\mathrm{Pr}_T(x) \equiv \exists y \mathrm{Prov}_T(y, x)$ の定義を与える．

はじめに証明のゲーデル数を定義しよう．理論 T における証明は論理式の有限列 $\varphi_0, \cdots, \varphi_n$ である．そこで

$$\beta(a, b, 0) = \ulcorner\varphi_0\urcorner, \quad \beta(a, b, 1) = \ulcorner\varphi_1\urcorner, \cdots, \beta(a, b, n) = \ulcorner\varphi_n\urcorner$$

となるような自然数 a, b を用いて

$$(\text{証明 } \varphi_0, \cdots, \varphi_n \text{ のゲーデル数}) = \mathrm{pair}(n, \mathrm{pair}(a, b))$$

と定義する (関数 pair の定義は 83 ページ参照)．どんな列 $\varphi_0, \cdots, \varphi_n$ に対してもこのような a, b が必ず存在することは β関数定理 (定理 4.24) によって保証され

いが，ここではこれで問題がない．）

次に論理式 $\mathrm{Prov}_T(y,x)$ の構成要素を順に定義していく．

自然数 x が項のゲーデル数であるならば，かつその時に限り，以下の (A)(B) を満たす自然数の有限列 $a_0,\cdots,a_n$ $(n \geqq 0)$ が存在する：

(A) $a_n = x$.

(B) 各 a_i について，以下の (1)〜(4) のどれかが成り立つ：

(1) a_i は 15 以上の奇数.

(2) $j<i$ なるある j について $a_i = \mathrm{pair}(1, a_j)$ となる.

(3) $j<i$ ならびに $k<i$ なるある j, k について $a_i = \mathrm{pair}(3, \mathrm{pair}(a_j, a_k))$ となる.

(4) $j<i$ ならびに $k<i$ なるある j, k について $a_i = \mathrm{pair}(5, \mathrm{pair}(a_j, a_k))$ となる.

この $a_0,\cdots,a_n$ は x が表す項の部分項のゲーデル数を並べたものである．(項のゲーデル数の定義は，$\ulcorner 0 \urcorner = 15$, $\ulcorner x \urcorner = 17$, $\ulcorner y \urcorner = 19, \cdots, \ulcorner \mathrm{S}(t) \urcorner = \mathrm{pair}(1, \ulcorner t \urcorner)$, $\ulcorner t+t' \urcorner = \mathrm{pair}(3, \mathrm{pair}(\ulcorner t \urcorner, \ulcorner t' \urcorner))$, $\ulcorner t \cdot t' \urcorner = \mathrm{pair}(5, \mathrm{pair}(\ulcorner t \urcorner, \ulcorner t' \urcorner))$ であった — 6.2 節参照．）さらに次のことが，関数 pair の定義と項のゲーデル数の定義からわかる：項 t のすべての部分項 (t 自身も含む) を $t_0,\cdots,t_n$ としたとき，

- $n < \ulcorner t \urcorner$,
- 各 i について $\ulcorner t_i \urcorner \leqq \ulcorner t \urcorner$.

(したがって $\ulcorner t \urcorner = \max\{n, \ulcorner t_0 \urcorner, \cdots, \ulcorner t_n \urcorner\}$ である．）以上のことと β関数定理によって,「x は項のゲーデル数である」を意味する PA の論理式 $\mathrm{Term}(x)$ を以下のように作れることがわかる：

$$\mathrm{Term}(x) \equiv \exists a < \gamma(x)\, \exists n < x (a_n = x \wedge \forall i \leqq n (B_1 \vee B_2 \vee B_3 \vee B_4)).$$

項 t に対して $a_t \equiv \beta(a, \delta(x), t)$.

$$B_1 \equiv (a_i \geqq \overline{15} \wedge \exists y < a_i\, (a_i = \overline{2} \cdot y + \overline{1})).$$

$$B_2 \equiv \exists j < i\, (a_i = \mathrm{pair}(\overline{1}, a_j)).$$

$$B_3 \equiv \exists j < i\, \exists k < i\, (a_i = \mathrm{pair}(\overline{3}, \mathrm{pair}(a_j, a_k))).$$

$$B_4 \equiv \exists j < i\, \exists k < i\, (a_i = \mathrm{pair}(\bar{5}, \mathrm{pair}(a_j, a_k))).$$

項 t, t' に対して $\mathrm{pair}(t,t') \;\equiv\; (t+t')\cdot(t+t'+\bar{1}) + \bar{2}\cdot t.$

関数 β, γ, δ などを表す論理式が Δ_1 であることと 5.5節の定理 5.9の直後の注意などによって，$\mathrm{Term}(x)$ は PA 上の Δ_1論理式であることがわかる．なお，この最後の略記法

$$\mathrm{pair}(t,t') \;\equiv\; (t+t')\cdot(t+t'+\bar{1}) + \bar{2}\cdot t$$

は以後ことわりなく使用する．

さらに，$\mathrm{Term}(x)$ を用いて同様の方法で「x は論理式のゲーデル数である」ということを意味する Δ_1論理式を作ることができるので，それを $\mathrm{Formula}(x)$ と記す．

さて，述語論理の公理は

$$\varphi{\to}(\psi{\to}\varphi), \quad (\varphi{\to}(\psi{\to}\theta)){\to}((\varphi{\to}\psi){\to}(\varphi{\to}\theta)), \cdots$$

推論規則は

三段論法 $\dfrac{\varphi \quad \varphi{\to}\psi}{\psi}$　　一般化法則 $\dfrac{\varphi{\to}\psi}{\varphi{\to}\forall x\psi}$ (ただし x は φ に現れない)

であった (30 ページ (2)(3)(4))．これらに対して，

- x は述語論理の公理 (Axiom) のゲーデル数である
- z は，ゲーデル数 x と ゲーデル数 y の論理式から三段論法 (Modus Ponens) によって得られた論理式のゲーデル数である
- y は，ゲーデル数 x の論理式から一般化法則 (Generalization) によって得られた論理式のゲーデル数である

をそれぞれ意味する PA 上の Δ_1論理式を作ることができるので，それらを $\mathrm{Ax}(x)$, $\mathrm{MP}(x,y,z)$, $\mathrm{Gen}(x,y)$ と記す．具体的には，たとえば $\mathrm{MP}(x,y,z)$ は

$$\mathrm{Formula}(z) \wedge y = \mathrm{pair}(\overline{11}, \mathrm{pair}(x,z))$$

であるし，$\mathrm{Ax}(x)$ は

$$\mathrm{Formula}(x) \wedge \exists a < x\, \exists b < x (x = \mathrm{pair}(\overline{11}, \mathrm{pair}(a, \mathrm{pair}(\overline{11}, \mathrm{pair}(b,a))))) \vee \cdots$$

である．(論理式のゲーデル数の定義は $\ulcorner \varphi{\to}\psi \urcorner = \mathrm{pair}(11, \mathrm{pair}(\ulcorner\varphi\urcorner, \ulcorner\psi\urcorner))$ であった．なお $\mathrm{Ax}(x)$ の定義の後半の “ $\cdots$ ” の部分では「論理式中の変数への項の代入」を Δ_1 で記述しなければならないので実際にはかなり複雑になる．)

入」を Δ_1 で記述しなければならないので実際にはかなり複雑になる．)

また同様にして「x は理論 Q の固有の公理のゲーデル数である」を意味する PA 上の Δ_1論理式をつくることもでき，それを $\mathrm{Ax_Q}(x)$ と記す．さらに，理論 T が RE 公理化可能であるならば，

$$\mathfrak{N} \models \mathrm{Ax}_T(\overline{n}) \Leftrightarrow n \text{ は } T \text{ の固有の公理のゲーデル数}$$

を満たす Q 上の Σ_1論理式 $\mathrm{Ax}_T(x)$ が存在することが補題 4.14(7) と再帰的関係の表現定理 (定理 5.6) によって簡単に示されるので，このような論理式 $\mathrm{Ax}_T(x)$ をひとつ固定しておく．

以上の準備のもとで，$\mathrm{Prov}_T(y,x)$ を次のように定義する．

$$\mathrm{Prov}_T(y,x) \ \equiv\ \exists n \leqq y\, \exists a \leqq y\, \exists b \leqq y\, (y = \mathrm{pair}(n, \mathrm{pair}(a,b)) \wedge x = a_n \wedge P).$$

項 t に対して $a_t \ \equiv\ \beta(a,b,t)$.

$$P \ \equiv\ \forall i \leqq n (\mathrm{Ax}_T(a_i) \vee \mathrm{Ax_Q}(a_i) \vee \mathrm{Ax}(a_i) \vee M \vee G).$$

$$M \ \equiv\ \exists j < i\, \exists k < i\, \mathrm{MP}(a_j, a_k, a_i).$$

$$G \ \equiv\ \exists j < i\, \mathrm{Gen}(a_j, a_i).$$

第二不完全性定理のための可証性述語 $\mathrm{Pr}_T(x)$ はこの Prov_T を使った論理式 $\exists y \mathrm{Prov}_T(y,x)$ であり，$\mathrm{Con}(T)$ はこの $\mathrm{Pr}_T(x)$ を使った文 $\neg\mathrm{Pr}_T(\overline{\ulcorner\bot\urcorner})$ である．

以上の定義から次のことはただちに言える：理論 T が Q の RE 拡大ならば論理式 $\mathrm{Pr}_T(x)$ が上のように定義できて，これは PA 上のΣ_1論理式であり，任意の論理式 φ に対して

$$T \vdash \varphi \ \Leftrightarrow\ \mathfrak{N} \models \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$$

(可証性述語としての当然の条件) を満たす．

注意． (1) 8.2節で注意した例 $T \vdash \neg\mathrm{Pr}^*_T(\overline{\ulcorner\bot\urcorner})$ からわかるように，第二不完全性定理のための可証性述語は適切に定義されなければならない．ただしここで「適切に」と言ったのは「$\mathrm{Prov}_T(y,x)$ はここで定義した論理式と寸分も違ってはいけない」ということではなく，「$\mathrm{Prov}_T(y,x)$ は『y は x の証明である』を素直に表したものであればよい」ということである．たとえばここでは論理の形式化の方法としてヒルベルト流の公理系を用いたが，これをゲンツェン流で行なうと「証

明のゲーデル数」が変わってくるのでそれに応じて別の可証性述語を作ることができる．するとこの新しい可証性述語を用いても，第二不完全性定理やそれに関連する議論をすべて同様に導くことができるのである．

(2) ここで定義した論理式 $\mathrm{Prov}_T(y,x)$ は T において関係 $\mathbf{Prov}_T(y,x)$ を表現する (87 ページの条件 (1)(2) が成り立つ) とは限らない．つまり Σ_1 論理式 $\mathrm{Ax}_T(x)$ の取り方によっては，$\mathbf{Prov}_T(n,m)$ が成り立たないにもかかわらず $T \nvdash \neg\mathrm{Prov}_T(\overline{n},\overline{m})$ であることがある (たとえば $\mathrm{Ax}_T(x) \equiv \mathrm{Pr}_{\mathrm{PA}}(x)$ という場合を考えてみよ．この T は RE 公理化可能で PA と同等な理論である)．ただしこの状況は 9.5節で説明する方法によって，ある意味では回避することができる．

9.3　可導性条件 D2 の証明

ここでは定理 8.1の中の **D2**, すなわち次を証明する．

定理 9.3 (可導性条件 D2) T が PA の RE 拡大ならば，任意の論理式 φ, ψ について

$$T \vdash (\mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner}) \land \mathrm{Pr}_T(\overline{\ulcorner\varphi\to\psi\urcorner})) \to \mathrm{Pr}_T(\overline{\ulcorner\psi\urcorner}).$$

[証明]　まず,「証明 P のゲーデル数 x と証明 Q のゲーデル数 y と論理式 ψ のゲーデル数 k をもらって，P と Q と ψ を順に並べた証明の最小のゲーデル数を返す」ような関数を $g(x,y,k)$ とする．(一つの証明に対してそのゲーデル数は複数存在するので，そのうちの最小値を返すようにしている．) ただし x や y がゲーデル数でないときには 0 を返すことにする．さて，

$$G(x,y,k,z) \quad \Leftrightarrow \quad z = g(x,y,k)$$

を意味する論理式 $G(x,y,k,z)$ を以下のように定義する：

$$G(x,y,k,z) \ \equiv \ G'(x,y,k,z) \land \forall z' < z \neg G'(x,y,k,z').$$

$$G'(x,y,k,z) \ \equiv \ A \lor B \lor C.$$

$$\begin{aligned}A \;\equiv\; & \exists n \exists a_x \exists b_x \exists m \exists a_y \exists b_y \exists a \exists b[\\ & \pi(x,n,a_x,b_x) \wedge \pi(y,m,a_y,b_y) \wedge \pi(z,n{+}m{+}2,a,b) \wedge \\ & \forall i \leqq n(\beta(a,b,i) = \beta(a_x,b_x,i)) \wedge \\ & \forall i \leqq m(\beta(a,b,n{+}1{+}i) = \beta(a_y,b_y,i)) \wedge \\ & \beta(a,b,n{+}m{+}2) = k\ ].\end{aligned}$$

$$\pi(t_0,t_1,t_2,t_3) \;\equiv\; (t_0 = \mathrm{pair}(t_1,\mathrm{pair}(t_2,t_3))).$$

$$B \;\equiv\; \neg\exists n \exists a_x \exists b_x\ \pi(x,n,a_x,b_x) \wedge (z=0).$$

$$C \;\equiv\; \neg\exists m \exists a_y \exists b_y\ \pi(y,m,a_y,b_y) \wedge (z=0).$$

すると，

$$\mathrm{PA} \vdash \forall x \forall y \forall k\ \exists! z\ G(x,y,k,z)$$

である．このことは

$$f(i,n,a_x,b_x,m,a_y,b_y,k) = \begin{cases} \beta(a_x,b_x,i),\ (i \leqq n \text{ のとき}), \\ \beta(a_y,b_y,i),\ ((n+1) \leqq i \leqq (n+m+1) \text{ のとき}), \\ \qquad k,\ (i \geqq (n+m+2) \text{ のとき}), \end{cases}$$

なる PA の項 $f(i,n,a_x,b_x,m,a_y,b_y,k)$ を使って，形式化された β関数定理 (定理 9.2) などによって示される．すると 3.4 節の系 3.11とその直後の議論によって PA には

$$g(x,y,k) = z \leftrightarrow G(x,y,k,z)$$

なる関数記号 g があるとしてよい．そして，論理式

$$\forall x \forall y((\mathrm{Prov}_T(x,\overline{\ulcorner\varphi\urcorner}) \wedge \mathrm{Prov}_T(y,\overline{\ulcorner\varphi\rightarrow\psi\urcorner}))\rightarrow\mathrm{Prov}_T(g(x,y,\overline{\ulcorner\psi\urcorner}),\overline{\ulcorner\psi\urcorner}))$$

が PA で証明できることを示せばよいが，このことは $G(x,y,k,z)$ の定義と Prov_T の定義からわかる．□

9.4 Σ_1完全性定理の形式化

ここでは定理 8.1の中の **D3** の証明に必要な次の定理を示す．

定理 9.4 (形式化された Σ_1完全性定理) 理論 T が PA の RE 拡大ならば，T 上

の任意の Σ_1文 φ に対して $T \vdash \varphi \to \mathrm{Pr}_T(\overline{\ulcorner \varphi \urcorner})$.

この定理の証明には多くの準備が必要である．まず関係「x は n を値とする数項のゲーデル数，すなわち

$$x = \ulcorner \overbrace{\mathrm{S}(\mathrm{S}(\cdots(}^{n\text{ 個}}0)\cdots)) \urcorner$$

である」を意味する PA の論理式 $\mathrm{Num}(n, x)$ を以下のように定義する：

$$\mathrm{Num}(n, x) \ \equiv\ \exists a \exists b \mathrm{N}(a, b, n, x).$$

$$\mathrm{N}(a, b, n, x) \ \equiv\ a_0 = \overline{15} \land a_n = x \land \forall i {<} n (a_{\mathrm{S}(i)} = \mathrm{pair}(\overline{1}, a_i)).$$

$$\text{項 } t \text{ に対して } a_t \ \equiv\ \beta(a, b, t).$$

すると次が成り立つ．

補題 9.5　$\mathrm{PA} \vdash \forall n\, \exists! x\, \mathrm{Num}(n, x)$.

[証明]　次の 2 つを示せば述語論理の推論によって補題は示される：

(1) $\mathrm{PA} \vdash \forall n\, \exists x\, \exists a\, \exists b\, \mathrm{N}(a, b, n, x)$.

(2) $\mathrm{PA} \vdash \forall n\, \forall x\, \forall x'\, \forall a\, \forall a'\, \forall b\, \forall b' ((\mathrm{N}(a, b, n, x) \land \mathrm{N}(a', b', n, x')) \to x = x')$.

どちらも PA の帰納法の公理 (n に関する帰納法) を用いて証明される．たとえば (1) を示すための「帰納法のステップ」のためには，a, b, k, x を自由変数として

$$\mathrm{PA} \vdash \mathrm{N}(a, b, k, x) \to \exists a'\, \exists b'\, \mathrm{N}(a', b', \mathrm{S}(k), \mathrm{pair}(\overline{1}, x))$$

を示せばよいが，このためには

$$f(i, y, a, b) = \begin{cases} \beta(a, b, i), & (i < y \text{ のとき}), \\ \mathrm{pair}(1, \beta(a, b, y-1)), & (i \geqq y \text{ のとき}), \end{cases}$$

なる関数 f が PA の項で扱えることを示してから，形式化された β関数定理 (定理 9.2) による

$$\mathrm{PA} \vdash \exists a'\, \exists b'\, \forall i {\leqq} \mathrm{S}(k) [\beta(a', b', i) = f(i, \mathrm{S}(k), a, b)]$$

を用いればよい．□

この補題と 3.4 節の系 3.11とその直後の議論によって PA は

$$\mathrm{num}(n) = x \leftrightarrow \mathrm{Num}(n, x)$$

なる関数記号 num を持つとする．

次に PA の項 t に対して，t と同じ自由変数を持つ PA の項 t^* を以下のように再帰的に定義する：

$$0^* \equiv \overline{15}.$$

x が変数のとき，$x^* \equiv \mathrm{num}(x)$.

t が項のとき，$\mathrm{S}(t)^* \equiv \mathrm{pair}(\overline{1}, t^*)$.

t_1 と t_2 が項のとき，$(t_1 + t_2)^* \equiv \mathrm{pair}(\overline{3}, \mathrm{pair}(t_1^*, t_2^*))$.

t_1 と t_2 が項のとき，$(t_1 \cdot t_2)^* \equiv \mathrm{pair}(\overline{5}, \mathrm{pair}(t_1^*, t_2^*))$.

自由変数 $x_1, \cdots, x_k$ を持つ項 $t(\overrightarrow{x})$ に対して $t(\overrightarrow{x})^*$ は $\ulcorner t(\overline{x_1}, \cdots, \overline{x_k}) \urcorner$ を意味する項になる．さらに同様にして，$x_1, \cdots, x_k$ を自由変数として持つ PA の論理式 $\varphi(\overrightarrow{x})$ に対して，同じ自由変数を持ち $\ulcorner \varphi(\overline{x_1}, \cdots, \overline{x_k}) \urcorner$ を意味する PA の項 $\varphi(\overrightarrow{x})^*$ が定義できる．束縛変数があるのでこの定義の正確な記述は少々面倒だが，次の例を見れば定義は明らかであろう：変数 x のゲーデル数が 17 であるとき，

$$(x = y)^* \equiv \mathrm{pair}(\overline{7}, \mathrm{pair}(\mathrm{num}(x), \mathrm{num}(y))).$$

$$(\forall x(x = y))^* \equiv \mathrm{pair}(\overline{13}, \mathrm{pair}(\overline{17}, \mathrm{pair}(\overline{7}, \mathrm{pair}(\overline{17}, \mathrm{num}(y))))).$$

(論理式のゲーデル数の定義は $\ulcorner a = b \urcorner = \mathrm{pair}(7, \mathrm{pair}(\ulcorner a \urcorner, \ulcorner b \urcorner))$, $\ulcorner \forall x \varphi \urcorner = \mathrm{pair}(13, \mathrm{pair}(\ulcorner x \urcorner, \ulcorner \varphi \urcorner))$ であった．)

さて，φ が文の場合は $T \vdash \varphi^* = \overline{\ulcorner \varphi \urcorner}$ となるので (定理 5.1(4))，次の補題から定理 9.4はただちに導かれる．

補題 9.6 (形式化された補題 5.5) 理論 T が PA の RE 拡大ならば，T上の任意の Σ_1論理式 φ に対して $T \vdash \varphi \rightarrow \mathrm{Pr}_T(\varphi^*)$.

[証明] 補題 5.5の証明と同じく φ が Σ_1 であることの定義に関する帰納法による．以下では Σ_1 の定義のうち三通りの場合だけを示す (残りも同様にできる)．

[φ が $t_1 = t_2$ の場合] いま次が成り立つ：

形式化された定理 5.1(4). t が PA の項であるとき

$$T \vdash \forall n(t = n \to \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(t^*, \mathrm{num}(n))))).$$

これによって

$$T \vdash \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(t_1^*, \mathrm{num}(t_1)))),$$

$$T \vdash \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(t_2^*, \mathrm{num}(t_2)))),$$

が成り立つ．ところで

$$T \vdash a = c, \quad T \vdash b = c \;\Rightarrow\; T \vdash a = b$$

を形式化した次も成り立つ：

$$T \vdash \forall x \forall y \forall z[\mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(x, z))) \wedge \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(y, z))) \to \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(x, y)))].$$

これは可導性条件 **D2** (定理 9.3) と同様に示すことができる．したがってこれらによって，

$$T \vdash t_1 = t_2 \to \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(t_1^*, t_2^*))),\ \text{すなわち}$$

$$T \vdash t_1 = t_2 \to \mathrm{Pr}_T((t_1 = t_2)^*)$$

が成り立つ．

[φ が $\forall x{<}t\psi$ の場合]　帰納法の仮定 ($T \vdash \psi \to \mathrm{Pr}_T(\psi^*)$) によって

$$T \vdash \forall x{<}t\psi \to \forall x(x < t \to \mathrm{Pr}_T(\psi^*)),$$

$$T \vdash \forall x{<}t\psi \to \forall n(t = n \to \forall x(x < n \to \mathrm{Pr}_T(\psi^*))),$$

である．ところで，いま次が成り立つ:

形式化された定理 5.3(c) の一部分．

$$T \vdash \forall n[\forall x(x{<}n \to \mathrm{Pr}_T(\psi^*)) \to \mathrm{Pr}_T((\forall x{<}n\psi)^*)].$$

したがって

$$T \vdash \forall x{<}t\psi \to \forall n(t = n \to \mathrm{Pr}_T((\forall x{<}n\psi)^*))$$

である．ここで，項 $(\forall x{<}n\psi)^*$ をこの中の num(n) の場所を指定して $f(\mathrm{num}(n))$ と記すと，この記法によって

$$T \vdash \forall x{<}t\psi \to \forall n(t = n \to \mathrm{Pr}_T(f(\mathrm{num}(n))))$$

となって，述語論理の推論によって

$$T \vdash \forall x{<}t\psi \to \mathrm{Pr}_T(f(\mathrm{num}(t)))$$

となる．ところで

$$T \vdash b = a, \quad T \vdash \forall x < a\, \psi \ \Rightarrow\ T \vdash \forall x < b\, \psi$$

を形式化した次も成り立つ：

$$T \vdash \forall x \forall y[\mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}(y, x))) \wedge \mathrm{Pr}_T(f(x)) \rightarrow \mathrm{Pr}_T(f(y))].$$

これは可導性条件 **D2** (定理 9.3) と同様に示すことができる．すると，この x に $\mathrm{num}(t)$ を，y に t^* を代入して，「形式化された定理 5.1(4)」などによって

$$T \vdash \forall x < t\, \psi \ \rightarrow\ \mathrm{Pr}_T(f(t^*)),$$ すなわち

$$T \vdash \forall x < t\, \psi \ \rightarrow\ \mathrm{Pr}_T((\forall x < t \psi)^*)$$

を得る．

[T上のΣ_1論理式 ψ に対して $T \vdash \varphi \leftrightarrow \psi$ の場合] いま

$$(\dagger) \quad T \vdash \mathrm{Pr}_T(\psi^*) \rightarrow \mathrm{Pr}_T(\varphi^*)$$

が言えれば，帰納法の仮定 ($T \vdash \psi \rightarrow \mathrm{Pr}_T(\psi^*)$) と $T \vdash \varphi \rightarrow \psi$ によって，求める

$$T \vdash \varphi \rightarrow \mathrm{Pr}_T(\varphi^*)$$

はただちに言える．(†) は $T \vdash \psi \rightarrow \varphi$ から可導性条件 **D2** (定理 9.3) と同様に証明できる．□

以上で補題 9.6が (したがって定理 9.4が) 証明されたが，厳密には「形式化された定理 5.1(4)」や「形式化された定理 5.3(c) の一部分」などを示さなければこの証明は完結しない．これらは基本的には 5.3節での議論をすべて T の中で形式化して行なえばよいのだが，実際にそれをやろうとすると，メタな立場では無意識に行なっていた議論をいちいち証明のゲーデル数の定義まで立ち帰って行なわなければならない．たとえば定理 5.1(2) をTの中で形式化して行なうとは

$$T \vdash \forall n \forall m\ \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}((n+m)^*, \mathrm{num}(n+m))))$$

(あるいは, $T \vdash \forall n \forall m\ \mathrm{Pr}_{\mathrm{Q}}(\cdots)$) を示すということである．これは，$n$ を自由変数として

$$\varphi(m) \ \equiv\ \mathrm{Pr}_T(\mathrm{pair}(\overline{7}, \mathrm{pair}((n+m)^*, \mathrm{num}(n+m))))$$

と置いて，

$$(\dagger) \quad T \vdash \varphi(0), \qquad (\ddagger) \quad T \vdash \forall m(\varphi(m) \rightarrow \varphi(\mathrm{S}(m)))$$

と帰納法の公理から求められるが，たとえば (‡) は，メタな立場で

$$T \vdash \overline{n} + \mathrm{S}(\overline{m}) = \mathrm{S}(\overline{n} + \overline{m}) = \mathrm{S}(\overline{n+m}) = \overline{n+m+1}$$

と行なった議論を形式化する必要がある．この一番目の等式変形に相当するのは

$$T \vdash \forall n \forall m\ \mathrm{Pr}_T((n + \mathrm{S}(m) = \mathrm{S}(n+m))^*)$$

であるが, これは「n と m をもらって T における $\overline{n} + \mathrm{S}(\overline{m}) = \mathrm{S}(\overline{n} + \overline{m})$ の証明のゲーデル数を返す関数 $g(n, m)$」が T の項として扱えることを，形式化された β関数定理などを使って可導性条件 **D2** (定理 9.3) の証明で行なったように示してから，

$$T \vdash \mathrm{Prov}_T(g(n, m), (n + \mathrm{S}(m) = \mathrm{S}(n+m))^*),$$

$$T \vdash \exists y\ \mathrm{Prov}_T(y, (n + \mathrm{S}(m) = \mathrm{S}(n+m))^*),$$

としなければならない．また三番目の等式変形に相当する部分では

$$T \vdash \mathrm{pair}(\overline{1}, \mathrm{num}(x)) = \mathrm{num}(\mathrm{S}(x))$$

が必要であり，これは関数 num の定義に戻って証明しなければならない．この調子で 5.3節での議論をすべて T の中で形式化して行なえば，求める補題 9.6は完全に証明される．しかし現実にはこれは非常に困難な作業である．

9.5　クレイグの手法の形式化

最後に，7.2節で説明した「クレイグの手法」を形式化して用いることについて説明しよう．

可証性述語の性質を詳細に調べる際に，論理式 $\mathrm{Prov}_T(y, x)$ が PA 上 (または T 上) で Δ_1 であれば都合が良いことが多い．(Δ_1論理式 $\mathrm{Prov}_T(y, x)$ は PA 上で関係 $\mathbf{Prov}_T(y, x)$ を表現することになる．9.2節の注意 (2) 参照．) このためには $\mathrm{Prov}_T(y, x)$ の定義に現れる論理式 $\mathrm{Ax}_T(x)$ が Δ_1 であればよいのだが，T が PA の RE 拡大のときに一般には $\mathrm{Ax}_T(x)$ は Δ_1 にならない．

しかしこのとき PA 上 の Δ_1論理式 $A(x, y)$ を用いて

$$\mathrm{Ax}_T(x) \equiv \exists y A(x, y)$$

とすることはできる (このことは補題 4.14(6) と定理 5.9からわかる)．また，自然

数上の 3 項関係

$$\mathbf{M}(a,b,c) \Leftrightarrow a\text{ は論理式 }(\varphi\text{ とする}) \text{ のゲーデル数であり，}$$
$$c = \ulcorner \overbrace{\varphi \wedge \varphi \wedge \cdots \wedge \varphi}^{b\text{ 個}} \urcorner$$

を表現する Δ_1論理式 $M(a,b,c)$ もある．そこでこれらを用いて，T と同等な理論 T' に対する $\mathrm{Ax}_{T'}(x)$ を

$$\mathrm{Ax}_{T'}(x) \equiv \exists a \leqq x\, \exists m \leqq x\, (M(a, m+1, x) \wedge A(a,m))$$

$$(\text{すなわち，}\exists \ulcorner\varphi\urcorner \leqq x\, \exists m \leqq x\, (x = \ulcorner \overbrace{\varphi \wedge \varphi \wedge \cdots \wedge \varphi}^{m+1} \urcorner \wedge A(\ulcorner\varphi\urcorner, m)))$$

と Δ_1 で作ることができる．そしてこれを用いて $\mathrm{Prov}_{T'}(y,x)$ そして可証性述語 $\mathrm{Pr}_{T'}(x)$ を作れば次が成り立つ．

(1) $\mathrm{Prov}_{T'}(y,x)$ は PA 上の Δ_1論理式．

(2) T と T' は同等であり，そのことを PA で証明できる．すなわち

$$\mathrm{PA} \vdash \forall x(\mathrm{Pr}_T(x) \leftrightarrow \mathrm{Pr}_{T'}(x)).$$

したがって，$\mathrm{Pr}_{T'}(x)$ の性質を (1) を用いて示しておいてから，そのことが $\mathrm{Pr}_T(x)$ に関しても成り立つことを (2) を用いて示せば,「T が PA の RE 拡大である」という条件のもとで可証性述語 $\mathrm{Pr}_T(x)$ のさまざまな性質 (たとえば 8.4節で説明した様相論理との関係) の証明を与えることができるのである．

パート B 参考文献

不完全性定理に関する本は数多く出版されているが，その中で定評ある教科書としてはパート A の参考文献 [8] および [10] (の中の不完全性定理の章) が挙げられる．この他にはパート B に関連するものとして

[1] G. Boolos, *The Logic of Provability*, Cambridge University Press (1993)

[2] C. Smoryński, *Self-Reference and Modal Logic*, Springer (1985)

がある．これらは 8.4節で説明した「不完全性定理と様相論理」に関する優れた教科書であり，様相論理ぬきの不完全性定理の部分だけでも読む価値がある．特に [1] には第二不完全性定理の証明が非常に詳細に書かれており，4.5, 4.6 節ならびにパート B を書くにあたって多いに参考にした．

Part C. 組合せ的独立命題

1977 年パリス (J. Paris) とハーリントン (L. Harrington) によって，PA で証明できない数学の定理 (独立命題) が発見された ([3])．ゲーデルが作った独立命題 Con(PA) はメタ数学的な内容であったので，それまで PA は普通の数学を扱う限り完全な体系であるという気分が残っていた．それを見事に打ち砕いたのがパリス-ハーリントンの仕事である．

このパート C ではパリス-ハーリントンの組合せ的命題 PH や，その他にヒドラ (Hydra)-ヘラクレス (Hercules) 戦やグッドシュタイン列 (R. Goodstein) についての組合せ的命題の独立性を示そう．

実際には，これらの命題は Π_2文で表現されるのだが (Con(PA) の方は Π_1文であった)，いま PA で証明できる Π_2文については，第 12 講のクライゼル (G. Kreisel) の定理によって急増加関数 F_α $(\alpha < \epsilon_0)$ による上限が与えられることがわかる．ところが，PH などの独立命題を表現する Π_2文から定義される関数は，この急増加関数の上限を越えてしまう．詳しく言うと，PA で証明できる Π_2文から定義される関数 f は，ある F_α $(\alpha < \epsilon_0)$ で支配される $(f \ll F_\alpha)$ ことがわかる．それゆえ PH などは PA で証明できなくなっているのである．

以上のような事情をこのパート C では詳しく見て行くことにしよう．具体的には次のようになる．

第 10 講では ϵ_0 までの順序数と急増加関数の基本的な性質を述べよう．

第 11 講では，弱い意味でのヒドラ-ヘラクレス戦とグッドシュタイン列の命題は，$I\Sigma_1$ (体系 Q に Σ_1論理式についての帰納法を加えたもの) で証明できないことを示す．そのためにパーソンズ (C. Parsons) の定理 (クライゼルの定理の $I\Sigma_1$ 版) を示そう．

第 12 講ではクライゼルの定理を証明する．そしてヒドラ-ヘラクレス戦とグッドシュタイン列の命題は，PA で証明できないことを示そう．

第13講では，パリス-ハーリントンの命題PHは真であるが，PAで証明できないことを示そう．また，PH(2)が$I\Sigma_1$で証明できないことも示す．

第 10 講　順序数と急増加関数

10.1　ϵ_0 までの順序数と基本列

独立性を示したい組合せ的命題を考えるために，ϵ_0 までの順序数とその基本列を定義しよう．

最初に ϵ_0 までの順序数を，自然数の構造をもとにして次のように定義しよう．まず自然数 $0, 1, 2, \cdots$ を並べおいて，そのあとに新しい数 ω をおく．

$$0,\ 1,\ 2,\ \cdots\ \omega$$

このとき ω はすべての自然数より大きい数と考えよう．自然数は 0 に 1 を次々と加えて得られることに着目して，ω にも次々と 1 を加えて並べよう．

$$0,\ 1, 2, \cdots\ \omega,\ \omega+1,\ \omega+2, \cdots.$$

そのあとに，より大きな数 $\omega+\omega$ をおく．この $\omega+\omega$ は $\omega\cdot 2$ と書いてもよい．さらに次々と 1 を加えて並べ，より大きい数 $\omega\cdot 2+\omega (=\omega\cdot 3)$ をおいて，ということを繰り返す．

$$0,\ 1,\ 2, \cdots\ \omega,\ \omega+1, \cdots\ \omega\cdot 2, \cdots\ \omega\cdot 3, \cdots\ \omega\cdot 4, \cdots.$$

さらにこれらより大きな数 $\omega\cdot\omega (=\omega^2)$ をおき，また 1 を次々に加えて並べる．これを繰り返すと次のような数が並ぶ．

$$0, 1, \cdots\ \omega, \cdots\ \omega\cdot 2, \cdots\ \omega^2, \cdots\ \omega^3, \cdots\ \omega^4, \cdots$$

またそのあとに ω^ω をおき，1 を次々と加える．この操作を繰り返してゆくと，結局

$$0, 1, \cdots\ \omega, \cdots\ \omega^\omega, \cdots\ \omega^{\omega+1}, \cdots\ \omega^{\omega^\omega}, \cdots$$

という数が並ぶであろう．この並びに出てくる数 α を ϵ_0 までの**順序数**とよぶ．以下では単に**順序数**とよび，$\alpha < \epsilon_0$ と書くことにする．つまり順序数は次の (1), (2) で再帰的に定義されるものとする．

定義．(1) 0 は最小の順序数である．

(2) $\alpha_1, \alpha_2, \cdots, \alpha_k$ が順序数で $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_k$ であるとき，

$$\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + \cdots + \omega^{\alpha_k}$$

も順序数である．ここで $\alpha \geqq \beta$ とは $\alpha > \beta$ または $\alpha = \beta$ のことであり，さらに $\alpha > \beta$ は指数部の辞書式順序で定まるものとする．つまり

$$\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_k}, \quad \beta = \omega^{\beta_1} + \cdots + \omega^{\beta_m}$$

とするとき，$\alpha > \beta$ とは次の (2a) または (2b) が成り立つときとする．

(2a) $k > m$ かつ $\alpha_1 = \beta_1, \cdots, \alpha_m = \beta_m$.

(2b) ある i に対し $\alpha_1 = \beta_1, \cdots, \alpha_{i-1} = \beta_{i-1}$, $\alpha_i > \beta_i$.

いま順序数について通常の略記法は自由に使うことにしよう．たとえば

$$\omega^0 = 1, \quad \omega^1 = \omega, \quad \omega^\alpha + \cdots + \omega^\alpha = \omega^\alpha \cdot n$$

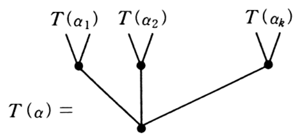
など．また順序数 α はその形から次の 3 つ場合に分けられることにも注意しよう．

(i) $\alpha = 0$ のとき．(ii) $\alpha = \beta + 1$ のとき．(iii) $\alpha = \beta + \omega^\delta$ $(\delta > 0)$ のとき (このとき α は極限数と呼ばれる)．

さらに順序数 α は，次の (1), (2) によって有限の木 $T(\alpha)$ としても表現される．

(1) $T(0) = \bullet$

(2) $\alpha = \omega^{\alpha_1} + \omega^{\alpha_2} + \cdots + \omega^{\alpha_k}$ のとき



例. (図 10.1)

逆に有限の木が与えられたとき，それを木表現にもつ順序数を作ることもできる (図 10.2)．

順序数の性質については，次の定理が重要である．

定理 10.1 順序数の無限下降列 $\alpha_0 > \alpha_1 > \alpha_2 > \cdots$ は存在しない．

[証明の概略] まず α_0 が自然数ならば，その下に無限下降列はない．また $\alpha_0 = \omega$ ならば α_1 が自然数だから，その下に無限下降列はない．同じように $\alpha_0 = \omega + n$

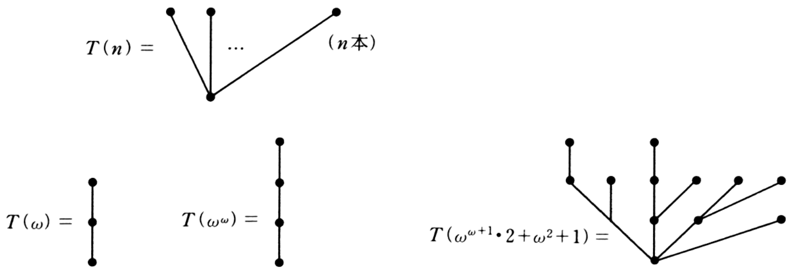


図 10.1

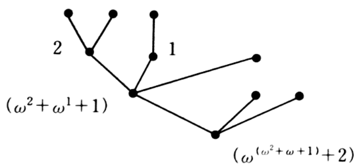


図 10.2

のときは $\alpha_n \leqq \omega$ だから，やはり無限下降列はないので，$\alpha_0 = \omega + \omega$ のときもその下に無限下降列はない．このような議論を続けてゆけば，すべての順序数の下に無限下降列はないことがわかる．□

この定理の主張は数学基礎論においてたいへん重要である．しかし，定理を証明することはそれを他の命題 (公理) に還元することであり，上の定理をさらに明らかな原理に分解するのはこの本の範囲を越えるので，ここではそれを公理として認めて進むことにしよう．さて，この定理からは帰納法の拡張版である次の超限帰納法の原理が導かれる．

超限帰納法の原理　$R(\alpha)$ を順序数 α についての関係とする．このとき次の (*) が示されれば，すべての α に対して $R(\alpha)$ が成り立つ．

(*) 任意の α に対して,「$\beta < \alpha$ に対する $R(\beta)$ は成り立っている」と仮定したとき $R(\alpha)$ も成り立つ.

[証明] もしこの原理が成り立たないとすると, $\neg R(\alpha_0)$ をみたす α_0 が存在し (*) をみたす. ここで (*) の α を α_0 とおけば, ((*) の対偶から) ある $\beta < \alpha_0$ で $\neg R(\beta)$ となるものが存在する. いま, $\beta = \alpha_1$ とおく. さらに α_1 についての (*) (の対偶) を考えると, $\alpha_2 < \alpha_1$ で $\neg R(\alpha_2)$ となるものがある. この議論を繰り返すと順序数の無限下降列 $\alpha_0 > \alpha_1 > \alpha_2 > \cdots$ ができる. これは定理 10.1 に矛盾するので, この原理が証明されたことになる. □

この超限帰納法の原理はよく関数の定義に使われる. たとえば「関数 $f(\alpha, x)$ が定義されている」という関係を考えれば, 超限帰納法により, $\beta < \alpha$ に対する $f(\beta, x)$ が定義されていると仮定して $f(\alpha, x)$ を定義すれば, すべての α に対して $f(\alpha, x)$ が定義されたことになる. この方法は原始再帰法による定義の拡張になっているので, **超限再帰法による定義**と呼ばれる.

さて順序数 α に対する**基本列** $\{\alpha[x] : x < \omega\}$ を次のように定義しよう. (これは $\alpha > 0$ ならば $\alpha > \alpha[x]$ となるので, α から始まる下降列を作るときに使われる.)

定義. (1) $\alpha = 0$ のとき $\alpha[x] = 0$.

(2) $\alpha = \beta + 1$ のとき $\alpha[x] = \beta$ (図 10.3).

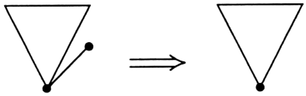


図 10.3

(3) $\alpha = \beta + \omega^{\gamma+1}$ のとき $\alpha[x] = \beta + \omega^{\gamma} \cdot (x+1)$ (図 10.4).

(4) $\alpha = \beta + \omega^{\delta}$ で δ が極限数のとき, $\alpha[x] = \beta + \omega^{\delta[x]}$.

(これは右上の部分木に対して定義を適用することを意味する.)

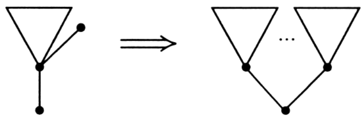


図 10.4

例. $\omega[x] = x + 1, \quad (\omega^{\omega})[x] = \omega^{x+1}, \quad (\omega^{\omega^{\omega}})[x] = \omega^{\omega^{x+1}}, \quad \cdots$

簡単のため，$(\alpha[x])[y]$ は $\alpha[x][y]$ と書くとしよう．基本列で大切なのは，順序数 $\alpha > 0$ と自然数の列 $x_1, x_2, \cdots$ が与えられたとき，順序数の下降列

$$\alpha > \alpha[x_1] > \alpha[x_1][x_2] > \cdots$$

ができることである．このとき定理 10.1 からこれは有限列となる．すなわち

$$\alpha > \alpha[x_1] > \alpha[x_1][x_2] > \cdots > \alpha[x_1][x_2]\cdots[x_m] = 0$$

となる m が必ず存在する．

注意. 順序数は有限の記号列にすぎないので，第 4 講と同じように自然数でうまくコード化できる．そして順序数上の $<$ や基本列などは，このコード化により自然数上の (原始再帰的な) 関係や関数として表される．さらに第 5 講の表現定理 (定理 5.8) を使えば，これらは算術の体系で表現されることがわかる．

10.2　ヒドラ-ヘラクレス戦

ヒドラはギリシャ神話に登場する 9 本首の怪物である．これをヘラクレスが退治するという話である．ヒドラは 1 本首を切られても新しい首を 2 本出すという強敵であった．実際にもヒドラと呼ばれる強力な自己復元，増殖能力を持つ微生物がいる．

ここではヒドラを有限の木と考え，上端点をヘッド，最下点をルートと呼ぶ．この戦いはヘラクレスがヒドラのヘッドを 1 回の攻撃で 1 個ずつ切り落として行き，ルートだけにしてしまえばヘラクレスの勝ちとする．ただしヒドラはヘラクレス

の攻撃の各回あとに，次のルールに従って成長する．

- 切られたヘッドの付け根から先の残っている部分が，それまでの攻撃の回数ぶんだけその下から増えてくる (図 10.5). (ただし，切られたヘッドの付け根がルートだと増えない．)

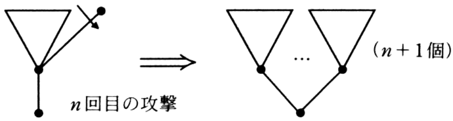


図 10.5

ヒドラはヘラクレスの攻撃の後ヘッドをどんどん増やしてゆく．しかしヒドラを木表現にもつ順序数を考えてみよう．各回戦の前の順序数 α_1 と後の順序数 α_2 に対して $\alpha_1 > \alpha_2$ となっている．だから定理 10.1 よりヘラクレスがどのような戦略をとっても有限回のうちにヒドラに勝つのである．特にヘラクレスが最も効率の悪いやり方

- ヘラクレスはつねにもっとも右端のヘッドを切る

という戦略で攻撃することを考えてみよう．このときのヒドラの情況を順序数で言うと，ヘラクレスの攻撃で次の下降列がつくられることを意味する．

$$\alpha > \alpha[1] > \alpha[1][2] > \alpha[1][2][3] > \cdots$$

この列は有限の長さで 0 となって止まる．すなわち次の命題が成り立つ．

命題 10.2 ヘラクレスはヒドラに必ず勝つ．

この命題は PA のΠ_2文で $\forall\alpha\ \exists y\ (\alpha[1][2]\cdots[y] = 0)$ と表現される．第 12 講では，これは PA で証明できない命題であることが示される．

例. $\alpha = \omega^\omega$ のとき $\alpha[1][2]\cdots[37] = 0$ (図 10.6).

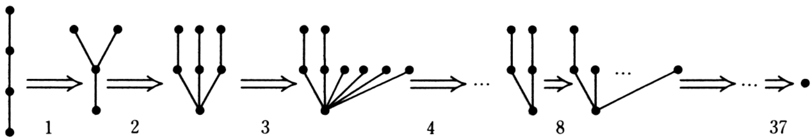


図 10.6

10.3　グッドシュタイン列

グッドシュタイン列は自然数を x-進法で表すことをうまく使って導き出す数列である．その停止性について不思議な現象が現れる．

まず，次のプロセス A を考えてみよう．これは自然数のペア (n, x) を入力して $(n', x+1)$ を出力するものである．

プロセス A　n と x が入力として与えられたとき，n を x 進法で表す．

$\Longrightarrow$ 表現の基底 x を $x+1$ にする．

$\Longrightarrow$ その数から 1 をひいたものを n' とする．

$\Longrightarrow$ n' と $x+1$ を出力する．

この出力を入力としてプロセス A を繰り返すことを考よう．こうして得られる数列 $n, n', n'', \cdots$ を弱グッドシュタイン列と呼ぶ．

例．$x = 2,\ n = \boxed{12} = 2^3 + 2^2$

$\Longrightarrow \quad n' = 3^3 + 3^2 - 1 = \boxed{35} = 3^3 + 2 \cdot 3 + 2$

$\Longrightarrow \quad n'' = 4^3 + 2 \cdot 4 + 2 - 1 = \boxed{71}$

$\Longrightarrow \quad n''' = 5^3 + 2 \cdot 5 + 1 - 1 = \boxed{135} \Longrightarrow \cdots$

次のプロセス B も自然数ペア (n, x) を入力して $(n', x+1)$ を出力するものである．

プロセス B　n と x が入力として与えられたとき，n を 純基底 x で表す (つまり n を x 進法で表し，その指数部も x 進法で表し，さらに指数部の指数部も x 進法で表し $\cdots$ と繰り返す)．

$\Longrightarrow$ 表現の純基底 x を $x+1$ にする.

$\Longrightarrow$ その数から 1 をひいたものを n' とする.

$\Longrightarrow$ n' と $x+1$ を出力する.

この出力を入力としてプロセス B を繰り返すことを考えよう. こうして得られる数列 $n, n', n'', \cdots$ をグッドシュタイン列と呼ぶ.

例. $x=2$, $n=\boxed{12}=2^{(2+1)}+2^2$

$$\Longrightarrow \quad n'=3^{(3+1)}+3^3-1=\boxed{107}=3^{(3+1)}+2\cdot 3^2+2\cdot 3+2$$

$$\Longrightarrow \quad n''=4^{(4+1)}+2\cdot 4^2+2\cdot 4+2-1=\boxed{1065}$$

$$\Longrightarrow \quad n'''=5^{(5+1)}+2\cdot 5^2+2\cdot 5+1-1=\boxed{15685} \Longrightarrow \cdots$$

この例で見る限りグッドシュタイン列は増加列のようだが, じつはどんな入力から始めても 0 に行き着くことが示されるのである. それは次のようにわかる.

まず順序数 α の表記のなかに現れる, すべての ω を $x+1$ に替えたものを $G_x(\alpha)$ とおく. さらに「順序数から 1 を引く」ことを意味する関数 P_x を

$$P_x(0)=0, \quad P_x(\alpha+1)=\alpha, \quad P_x(\alpha)=P_x(\alpha[x]) \ (\alpha \text{ が極限数})$$

により超限再帰法で定義する. すると $G_x(P_x(\alpha))=G_x(\alpha)-1$ がわかるので, 下の例からわかるように, グッドシュタイン列 $n, n', n'', \cdots$ は順序数の下降列

$$\alpha > P_x(\alpha) > P_{x+1}(P_x(\alpha)) > \cdots$$

に対応づけられる.

例.

$$\begin{array}{lcl} n=x^x+x & \overset{G_{(x-1)}}{\longleftarrow} & \alpha=\omega^\omega+\omega \\ \downarrow \boxed{\text{プロセス B}} & & \downarrow \ P_x \\ n'=(x+1)^{(x+1)}+(x+1)-1 & \overset{G_x}{\longleftarrow} & P_x(\alpha)=\omega^\omega+(x+1)-1 \end{array}$$

定理 10.1 により順序数の下降列は有限だから, 結局次が成り立つ.

命題 10.3 グッドシュタイン列は必ず 0 に行き着く.

この命題は PA の Π_2文で次のように表現される．

$$\forall\alpha\forall x\,\exists y\,(P_y(\cdots P_{x+1}(P_x(\alpha))\cdots)=0)$$

これも第 12 講で PA で証明できない命題であることが示される．

10.4　急増加関数

急増加関数 F_α $(\alpha<\epsilon_0)$ は第 12 講でみるように，PA で証明できる Π_2文の上限を与えるものとなる．これは超限再帰法で次のように定義される自然数上の 1 変数関数である．

$$F_0(x)=x+1,\qquad F_{\alpha+1}(x)=F_\alpha^{x+1}(x),\qquad F_\lambda(x)=F_{\lambda[x]}(x)$$

ただし λ は極限数を表し，$F_\alpha^{x+1}(x)$ は x に F_α を $x+1$ 回ほどこしたもの，すなわち $F_\alpha^{x+1}(x)=F_\alpha(\cdots(F_\alpha(x))\cdots)$ とする．

例. $F_1(x)=F_0(\cdots(F_0(x))\cdots)=(x+1)+1\cdots+1=2x+1.$

$F_2(x)=2\cdots(2(2x+1)+1)\cdots+1=2^{x+1}\cdot x+2^{x+1}-1.$

$F_3(x)\geqq 2^{\cdot^{\cdot^{2^x}}}$ ($x+1$ 個の 2)

急増加関数の性質を考えよう．自然数上の 1 変数関数 f,g に対して，ある m があって，$m<x$ ならば $f(x)<g(x)$ が成り立つとき，g は f を**支配する**といい $f\ll g$ と書く．これは g が f よりも急増加することを意味している (図 10.7)．

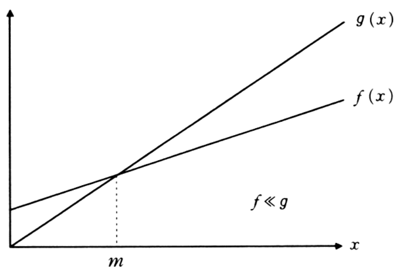


図 10.7

また f が k 変数のときにも，ある m があって $m < \max\{x_1, \cdots, x_k\}$ ならば

$$f(x_1, \cdots, x_k) < g(\max\{x_1, \cdots, x_k\})$$

であるとき g は f を支配するといい $f \ll g$ と書こう．このとき次が成り立つ．

定理 10.4 (1) F_α は単調増加である．

(2) $\alpha < \beta$ ならば，ある $k < \omega$ に対して $\alpha <_k \beta$.

(ただし $\alpha <_k \beta$ は，$\alpha < \beta$ かつ $\beta[k][k] \cdots [k] = \alpha$ (有限個の k) のこと．)

(3) $\alpha <_k \beta$ ならば $F_\alpha(x) \leqq F_\beta(x)$ $(x \geqq k)$.

だから，$\beta < \alpha$ ならば $F_\beta \ll F_\alpha$ が成り立つ．

(4) $F_\alpha \ll F_{\epsilon_0}$ $(\alpha < \epsilon_0)$.

(ただし F_{ϵ_0} は $F_{\epsilon_0}(x) = F_{\gamma_x}(x)$, $\gamma_x = \omega^{\cdot^{\cdot^{\omega}}}$ (x 個の ω) で定義される．)

この定理の証明は α についての超限再帰法を使ってできるが，ここでは演習問題としよう．次に，特に F_ω については次の定理に注意しよう．

定理 10.5 原始再帰的関数 f に対し $f \ll F_n$ となる $n < \omega$ が存在する．だから $f \ll F_\omega$ が成り立つ．

[証明] f の構成に関する帰納法で示そう．初期関数 (Z, S(x), P^n_i) についてはすべて $\ll F_1$ だからよい．また，f が合成 $f(x) = g(h(x))$ で定義されたときは，帰納法の仮定から $g \ll F_n$, $h \ll F_m$ となる n, $m < \omega$ が存在する．このとき $r = \max\{n, m\}$ とおけば $g, h \ll F_r$ だから，十分大きな x に対して

$$f(x) = g(h(x)) < F_r(F_r(x)) < F_r^{x+1}(x) = F_{r+1}(x)$$

が成り立つので $f \ll F_{r+1}$ となる．また，f が原始再帰法 $f(\overrightarrow{x}, 0) = g(\overrightarrow{x})$, $f(\overrightarrow{x}, y+1) = h(\overrightarrow{x}, y, f(\overrightarrow{x}, y))$ で定義されたときは，合成のときと同様に $g, h \ll F_r$ となる r が存在する．このとき十分大きな m をとれば，

$$m < \max\{\overrightarrow{x}, y\} \quad \text{ならば} \quad f(x, y) < F_r^{y+1}(x)$$

であることが y の帰納法で示される．だからこのとき $f(x, y) < F_{r+1}(\max\{x, y\})$ が成り立つので $f \ll F_{r+1}$ となる．□

次に F_α とヒドラ-ヘラクレス戦の関係を考えよう．まず $(\alpha+x)[1][2]\cdots[x]=\alpha$ は容易にわかるから，命題 10.2 (ヘラクレスはヒドラに必ず勝つ) を表現する Π_2 文は

$$\forall\alpha\forall x\,\exists y\,(\alpha[x+1][x+2]\cdots[y]=0)$$

と考えてよい．そこで次の関数 $H_\alpha(x)$ が自然に定義される．

$$H_0(x)=x,\quad H_\alpha(x)=\mu y(\alpha[x+1][x+2]\cdots[y]=0)\ \ (\alpha>0)$$

(ただし $\mu y(\cdots)$ は $(\cdots)$ をみたす最小の y のこと．) この関数はヘラクレスがヒドラ $\alpha+x$ に何回の攻撃で勝つか，その最小値を表している．性質としては，

$$H_\alpha(x)=H_{\alpha[x+1]}(x+1),\quad H_{\alpha+\beta}(x)=H_\alpha(H_\beta(x))$$

がある．(前者は $H_\alpha(x)$ の定義から容易．後者は β の超限再帰法によって示される．) この関数と急増加関数については次が成り立つ．

定理 10.6　$F_\alpha(x)\leqq H_{\omega^\alpha}(x)$.

[証明]　α の超限帰納法で示そう．まず $\alpha=0$ のときは，$F_0(x)=x+1=H_1(x)$ だからよい．次に $\alpha=\beta+1$ のときは，超限再帰法の仮定より

$$(F_\alpha(x)=)\ \ F_\beta^{x+1}(x)\leqq H_{\omega^\beta}^{x+1}(x)\ (=H_{\omega^\beta\cdot(x+1)}(x))$$

であり，次が成り立つのでよい．

$$F_\alpha(x)\leqq H_{\omega^\beta\cdot(x+1)}(x)\leqq H_{\omega^\beta\cdot(x+2)}(x+1)=H_{\omega^\alpha}(x).$$

また α が極限数のときも超限再帰法の仮定から次が成り立つのでよい．

$$F_\alpha(x)\leqq F_{\alpha[x+1]}(x+1)\leqq H_{\omega^{\alpha[x+1]}}(x+1)=H_{\omega^\alpha}(x).\quad\square$$

命題 10.3 (グッドシュタイン列は必ず 0 に行き着く) についても同様に，次の関数 D_α が定義できる．

$$D_0(x)=x,\quad D_\alpha(x)=\mu y(P_y(\cdots P_{x+2}(P_{x+1}(\alpha))\cdots)=0)\ (\alpha>0)$$

これは，入力 $(x,G_x(\alpha))$ として始めたグッドシュタイン列が 0 に行き着いて $(y,0)$ を出力するときの y を表す．このとき H_α のときと同様にして次が示される．

定理 10.7　$F_\alpha(x)\leqq D_{\omega^\alpha}(x)$.

以下の 2 つの講では，これらの不等式を使って命題 10.2 (ヘラクレスはヒドラに必ず勝つ) と命題 10.3 (グッドシュタイン列は必ず 0 に行き着く) の独立性を示すことにしよう．

第 11 講 パーソンズの定理 ($I\Sigma_1$ と原始再帰的関数)

11.1 パーソンズの定理の応用

パーソンズの定理を使って，弱い意味でのヒドラ-ヘラクレス戦と弱グッドシュタイン列の命題が，$I\Sigma_1$ (体系 Q に Σ_1論理式についての帰納法を加えたもの) で証明できないことを示そう．パーソンズの定理の証明は次の節以降で行う．ここでは簡単のため，Σ_1論理式とは $\exists y_1 \cdots \exists y_k \theta(\overrightarrow{x}, y_1, \cdots, y_k)$ (θ は有界論理式) のこととしよう．

定理 11.1 **(パーソンズ)** $\forall x_1 \cdots \forall x_n \exists y\, \phi(x_1, \cdots, x_n, y)$ (ϕ は Σ_1) が $I\Sigma_1$ で証明できるとする．このとき

$$\forall x_1 \cdots \forall x_k \exists y < f(x_1, \cdots, x_n)\ (\phi(x_1, \cdots, x_n, y))$$

が真となるような原始再帰的な関数 f が存在する．

このパーソンズの定理は，$I\Sigma_1$ で証明できる Π_2文 $\forall \overrightarrow{x}\ \exists y\, \phi(\overrightarrow{x}, y)$ から定義される関数 $g(\overrightarrow{x}) = \mu y(\phi(\overrightarrow{x}, y)$ が真) が，原始再帰的な f によって上から押さえられることを意味している．このとき定理 10.5 によれば，g はある急増加関数 F_n ($n < \omega$) で支配される．だから $g \ll F_\omega$ である (図 11.1)．また g は原始再帰的となることも第 4 講の結果 (補題 4.5) からわかる．

いま「ヘラクレスはヒドラ $T(\alpha)(\alpha < \omega^\omega)$ に勝つ」という命題を考えてみよう．これは $\forall \alpha < \omega^\omega\ \exists y\, (\alpha[1][2] \cdots [y] = 0)$ という Π_2文で表現される (命題 10.2)．もしこれが $I\Sigma_1$ で証明できるとすると，特に $(\omega^m + x)[1][2] \cdots [x] = \omega^m$ だから

$$\forall m\, \forall x\, \exists y\, (\omega^m[x+1][x+2] \cdots [y] = 0)$$

が証明できるはずである．したがってパーソンズの定理から m, x の関数

$$H_{\omega^m}(x) = \mu y(\omega^m[x+1][x+2] \cdots [y] = 0)$$

は，ある F_n で支配される．特に $m = n$ とおけば $H_{\omega^n} \ll F_n$. ところが定理 10.6

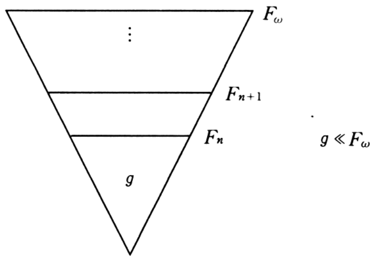


図 11.1

から $F_n \ll H_{\omega^n}$ だから矛盾である．したがってこの命題は $\mathrm{I}\Sigma_1$ で証明できない．

また「弱グッドシュタインは 0 に行き着く」という命題についても同様に，もし $\mathrm{I}\Sigma_1$ で証明できるとすると，パーソンズの定理と定理 10.7 から矛盾が導かれる．だからこれも $\mathrm{I}\Sigma_1$ で証明できない．以上のことをまとめると，次のようになる．

定理 11.2 (1) 命題「ヘラクレスはヒドラ $T(\alpha)(\alpha < \omega^\omega)$ に勝つ」は $\mathrm{I}\Sigma_1$ で証明できない．

(2) 命題「弱グッドシュタイン列は 0 に行き着く」は $\mathrm{I}\Sigma_1$ で証明できない．

11.2 $\mathrm{I}^*\Sigma_1$

パーソンズの定理の証明のために，$\mathrm{I}\Sigma_1$ を含んでいて，より扱いやすい体系 $\mathrm{I}^*\Sigma_1$ を定義しておこう．パーソンズの定理は 11.3 節で $\mathrm{I}^*\Sigma_1$ の証明の長さについての帰納法で示されることになる．

定義. $\mathrm{I}^*\Sigma_1$ は次の (1)〜(6) で定義される．

(1) $\mathrm{I}^*\Sigma_1$ の定数記号は 0 で，関数記号は原始再帰的関数 f の各定義に対しての記号 f すべてとする．($\mathrm{S}(x)$, P^n_j, $+$, $\cdot$ など．)

(2) 関係記号は等号 $=$ とその否定を表す $\neq$ とする．

(3) 論理記号は $\wedge, \vee, \forall, \exists, \forall x < t, \exists x < t$ とする．

有界量化記号 $\forall x < t(\cdots)$, $\exists x < t(\cdots)$ は通常どおりそれぞれ $\forall x(x < t \to (\cdots))$, $\exists x(x < t \land (\cdots))$ と解釈される．ただし t は x を含まない項とする．また有界論理式とは非有界な量化記号 $\forall, \exists$ を含まないものをいう．

否定を表す論理記号 $\neg$ はない．しかし否定文 $\neg\phi$ は以下の法則を使えば，原子文 $s = t$, $s \neq t$ から (3) の論理記号だけで構成できる．

$\neg\neg\phi = \phi$, $\neg(\phi \lor \psi) = \neg\phi \land \neg\psi$, $\neg(\phi \land \psi) = \neg\phi \lor \neg\psi$,

$\neg\forall\phi = \exists\neg\phi$, $\neg(\forall x < t)\phi = \exists x < t(\neg\phi)$ など.

(4) $\mathrm{I}^*\Sigma_1$ では「論理式の有限集合の証明」を考える．

論理式の有限集合 $\{\phi_1, \cdots, \phi_n\}$ は実際には $\phi_1 \lor \cdots \lor \phi_n$ を意味している．いま考える論理は一階述語論理なので，同じ論理式の重複や論理式の並びの順番などは気にしないでおきたいために，有限集合の記法が特に便利なのである．簡単のため集合 $\{\phi_1, \cdots, \phi_n\}$ を $\phi_1, \cdots, \phi_n$ と表すことにする．

(5) $\mathrm{I}^*\Sigma_1$ の証明とは，次のような公理から出発して，(6) で述べる推論規則を有限回使って得られる図形のことである．これは各点に論理式の集合を貼りつけた木の形をしている．その公理は次のものとする．(ただし，f は関数記号，$t, u, \cdots$ は項を表す．以下の公理は，記法としては複雑になっているが，$\neg\phi_1, \phi_2$ は $\phi_1 \to \phi_2$ を意味していることに注意すれば，どれも通常の公理を述べていることがわかる．)

(排中律)　$\neg\psi(\overrightarrow{t})$, $\psi(\overrightarrow{t})$ (ただし ψ は有界論理式とする).

(等号の公理)　$t = t$　　$t \neq u, u = t$　　$t \neq u, u \neq w, t = w$

$$t_1 \neq u_1, \cdots, t_k \neq u_k,\ f(t_1, \cdots, t_k) = f(u_1, \cdots, u_k)$$

(Q の公理 A1-A3) $\mathrm{S}(t) \neq \mathrm{S}(u), t = u$　　　$\mathrm{S}(t) \neq 0$

$$t = 0,\ \exists x < t(t = \mathrm{S}(x))$$

(原始再帰的関数 f の定義式)

(+ の定義) $t + 0 = t$　　$t + \mathrm{S}(u) = \mathrm{S}(t + u)$

($\cdot$ の定義) $t \cdot 0 = 0$　　$t \cdot \mathrm{S}(u) = t \cdot u + t$

その他の原始再帰的関数も同様に定義される．

(6) $\mathrm{I}^*\Sigma_1$ の推論規則は次のものとする．(ただし Γ, Δ は論理式の有限集合を表

す．Γ, ψ は $\Gamma \cup \{\psi\}$ のこととする．）

$$(\vee)\ \frac{\Gamma, \phi}{\Gamma, \phi \vee \psi} \qquad \frac{\Gamma, \psi}{\Gamma, \phi \vee \psi} \qquad (\wedge)\ \frac{\Gamma, \phi \quad \Gamma, \psi}{\Gamma, \phi \wedge \psi}$$

$$(\text{増})\ \frac{\Gamma}{\Delta}\ \text{ただし}\ \Gamma \subseteqq \Delta \quad (\exists)\ \frac{\Gamma, \phi(t)}{\Gamma, \exists x\ \phi(x)} \quad (\forall)\ \frac{\Gamma, \phi(z)}{\Gamma, \forall x\ \phi(x)}$$

$$(\exists <)\ \frac{\Gamma, \phi(u)}{\Gamma, \neg u < t, \exists x < t\ (\phi(x))} \qquad (\forall <)\ \frac{\Gamma, \neg z < t, \phi(z)}{\Gamma, \forall x < t\ (\phi(x))}$$

ただし $(\forall)$ と $(\forall <)$ の z はその推論規則の下式に現れない自由変数

$$(\text{カット})\ \frac{\Gamma, \neg\phi \quad \Delta, \phi}{\Gamma \cup \Delta}\ (\phi\ \text{はカット論理式とよばれる})$$

$$(\Sigma_1\ \text{帰納法規則})\ \frac{\Gamma, \phi(0) \quad \Gamma, \neg\phi(x), \phi(\mathrm{S}x)}{\Gamma, \phi(t)}$$

ただし $\phi(x)$ は Σ_1論理式であり，上式の x は下式には現れないとする．

この $\mathrm{I}^*\Sigma_1$ が $\mathrm{I}\Sigma_1$ を含むことは次のようにわかる．$\mathrm{I}^*\Sigma_1$ は Q の公理を含むことは明らか．排中律は，$\mathrm{I}^*\Sigma_1$ には有界論理式についてのみあるが，一般の論理式について証明できる．(たとえば ϕ と ψ の排中律から $\phi \vee \psi$ の排中律が次のように導かれる．他の論理記号の場合も同様である．)

$$(\vee)\ \cfrac{(\wedge)\ \cfrac{\neg\phi, \phi \quad \neg\psi, \psi}{\neg\phi \wedge \neg\psi,\ \phi,\ \psi}}{(\vee)\ \cfrac{\neg\phi \wedge \neg\psi,\ \phi,\ \phi \vee \psi}{\neg\phi \wedge \neg\psi,\ \phi \vee \psi}}$$

また Σ_1 帰納法の公理 $\phi(0) \wedge \forall x(\phi(x) \to \phi(\mathrm{S}(x))) \to \forall z\ \phi(z)$ (ただし ϕ は Σ_1) も証明できる．これを示すために

$$\{\neg\phi(0), \exists x(\phi(x) \wedge \neg\phi(\mathrm{S}(x)))\}$$

を Γ とおく．排中律から $\Gamma, \phi(0)$ と $\Gamma, \neg\phi(x), \phi(\mathrm{S}(x))$ がすぐに証明できるので，$\mathrm{I}^*\Sigma_1$ の Σ_1 帰納法規則と $(\forall)$ 規則より $\Gamma, \forall x\ \phi(x)$ が証明できる．これは Σ_1 帰納法の公理を表している．だから $\mathrm{I}^*\Sigma_1$ は $\mathrm{I}\Sigma_1$ を含むことがわかった．

11.3 カット消去定理

パーソンズの定理を示すため，$\mathrm{I}^*\Sigma_1$ のカット消去定理を考察しよう．

定理 11.3 (カット消去定理) I$^*\Sigma_1$ で Γ の証明があるとする．このときカット論理式が Σ_1 とならないカットは消去できる．(すなわち，含まれるカット論理式はすべて Σ_1 であるような Γ の証明が存在する．) (図 11.2)

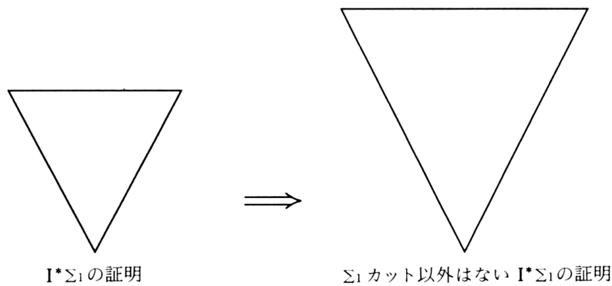


図 11.2

[証明の概略] ゲンツェンによるカット消去法で Σ_1 以外のカット論理式をもつカット規則を消去する．このカット消去法は証明論の基本となる方法である．ここでは要点のみ述べることにしよう．(詳しくは竹内-八杉 [4] などを参照．) それは Σ_1 以外のカット論理式をもつ証明を，より簡単な証明に書きかえるところにある．たとえば Γ が次のように導かれた場合を考えよう．(ここで証明 P_1, P_2 には Σ_1 以外のカット論理式はないとする．)

$$\text{(カット)}\dfrac{(\forall)\dfrac{\begin{matrix}\vdots\ P_1\\ \Gamma,\ \forall x\,\neg\phi(x),\ \neg\phi(z)\end{matrix}}{\Gamma,\ \forall x\,\neg\phi(x)} \qquad (\exists)\dfrac{\begin{matrix}\vdots\ P_2\\ \Delta,\ \exists x\,\phi(x),\ \phi(t)\end{matrix}}{\Delta,\ \exists x\,\phi(x)}}{\Gamma\cup\Delta}$$

この証明を次のような,「より簡単な」証明に書きかえる．

$$\dfrac{\dfrac{\begin{matrix}\vdots\ P_1'\\ \Gamma,\ \forall x\,\neg\phi(x),\ \neg\phi(t)\end{matrix} \qquad \dfrac{\begin{matrix}\vdots\ P_2\\ \Delta,\exists x\,\phi(x),\phi(t)\end{matrix}}{\Delta,\ \exists x\,\phi(x)}}{\Gamma\cup\Delta,\ \neg\phi(t)} \qquad \dfrac{\begin{matrix}\vdots\ P_2\\ \Delta,\ \exists x\,\phi(x),\ \phi(t)\end{matrix} \qquad \dfrac{\begin{matrix}\vdots\ P_1\\ \Gamma,\forall x\,\neg\phi(x),\neg\phi(z)\end{matrix}}{\Gamma,\ \forall x\,\neg\phi(x)}}{\Gamma\cup\Delta,\ \phi(t)}}{\Gamma\cup\Delta}$$

ただし証明 P_1' は P_1 の z に t を代入したもの．この書きかえで証明が「より

簡単」になっているのは，新しい証明の 3 つのカットはどれも前の証明のカットより，左上にくる証明の長さか，あるいはカット論理式の長さが短くなっていることからわかる．このような証明の書きかえを有限回おこなって，結局 Σ_1 以外のカット論理式は消去できる．□

上の状況で，もし $\Gamma, \exists x\, \phi(x)$ が $(\exists)$ ではなく，帰納法で導出されているときには書きかえはうまく行かない，だから $\mathrm{I}^*\Sigma_1$ では Σ_1 カット論理式のカットは消去できない．また一般の論理式に対する帰納法をもつ PA では，そのままではカット消去はできないわけで，第 12 講では PA のカット消去について新たな工夫を考える．

11.4 パーソンズの定理の証明

この証明のアイデアは Σ_1論理式に解釈 $\models$ を与えることにある．まず，Σ_1論理式 $\phi(\overrightarrow{x}) = \exists y_1 \cdots \exists y_k\, \theta(\overrightarrow{x}, y_1, \cdots, y_k)$ (θ は有界論理式) に対して，

$$\exists y_1 < n \cdots \exists y_k < n\ \ \theta(\overrightarrow{m}, y_1, \cdots, y_k)$$

が真であるとき

$$n \models \phi(\overrightarrow{m})$$

と書く．さらに Σ_1論理式の集合 $\Gamma(\overrightarrow{x}) = \{\phi_1(\overrightarrow{x}), \cdots, \phi_r(\overrightarrow{x})\}$ に対しては，$n \models \phi_i(\overrightarrow{m})$ が成り立つ $i (1 \leqq i \leqq r)$ が存在するとき次のように書く．

$$n \models \Gamma(\overrightarrow{m}).$$

この $\models$ には $<$-保存性 ($n \models \Gamma(\overrightarrow{m})$ かつ $n < n'$ ならば $n' \models \Gamma(\overrightarrow{m})$) があることに注意しよう．

さらに Π_2論理式の解釈についても考えよう．Π_2論理式とは

$$\psi = \forall x_1 \cdots \forall x_m\, \exists y_1 \cdots \exists y_k\, \theta(x_1, \cdots x_m, y_1, \cdots, y_k)$$

(θ は有界論理式) のこととする．このとき論理式 $\psi^\star(\overrightarrow{z})$ を

$$\psi^\star(\overrightarrow{z}) = \exists y_1 \cdots \exists y_k\, \theta(\overrightarrow{z}, y_1, \cdots, y_k)$$

と定義する．ただし $\overrightarrow{z} = z_1, \cdots, z_m$ は ψ に現れない新しい変数．$\psi^\star(\overrightarrow{z})$ は Σ_1

論理式となる．Π_2論理式の集合 $\Gamma = \{\psi_1, \cdots, \psi_n\}$ に対しては，

$$\Gamma^\star(\overrightarrow{z_1}, \cdots, \overrightarrow{z_n}) = \{\psi_1^\star(\overrightarrow{z_1}), \cdots, \psi_n^\star(\overrightarrow{z_n})\}$$

と定義する．ただし導入される新しい変数はすべて相異なるものとする．$\Gamma^\star$ は Σ_1 論理式の集合となるので，それに対する上記の解釈を Γ の解釈と考えよう．

さてパーソンズの定理は次を示せば十分であることは容易にわかる．(次の定理で，$\Gamma = \{\forall \overrightarrow{x}\, \exists y\, \phi(\overrightarrow{x}, y)\}$ とおけばよい．)

定理 11.4　Π_2論理式の集合 Γ が $I^*\Sigma_1$ で証明できるとする．このとき原始再帰的な f が存在して，すべての $\overrightarrow{m}$ で $f(\overrightarrow{m}) \models \Gamma^\star(\overrightarrow{m})$ となる．

[証明]　Γ が $I^*\Sigma_1$ で証明できるとしよう．カット消去定理から，カット論理式がすべて Σ_1 である Γ の証明 $\mathcal{P}$ がある．いま $\mathcal{P}$ に含まれる論理式は Π_2 である．なぜなら Γ 内の論理式はすべて Π_2 で，Γ に入っていない $\mathcal{P}$ の論理式は，Γ 内の論理式の部分式か，カット論理式であるから．

そこで $\mathcal{P}$ の長さ (使われた推論規則の数) の帰納法で f の存在を示そう．以下の論議では f, g, h などは原始再帰的で各変数について狭義に単調増加とする．

(1) Γ が公理のとき．Γ は非有界な $\forall, \exists$ を含まないから，どんな f をとっても成り立つ．たとえば $f(\overrightarrow{x}) = x_1 + \cdots + x_k$.

次に各推論規則について，上式について仮定して，下式に対する f の存在を示そう．(簡単のため $\Gamma^\star = \Gamma$, $\phi^\star = \phi$, $\overrightarrow{x} = x$ としよう．)

(2) $(\wedge)$ で Γ, ϕ と Γ, ψ から $\Gamma, \phi \wedge \psi$ が導かれているとき．仮定から次をみたす g, h がある．

$$g(m) \models \Gamma(m), \phi(m). \quad h(m) \models \Gamma(m), \psi(m).$$

だから $\max\{g(x), h(x)\} \leqq f(x)$ をみたす f をとれば求める式

$$f(m) \models \Gamma(m), \phi \wedge \psi(m)$$

が得られる．$(\vee)$ のときも同様．

(3) (増) のときは明らか．

(4) $(\exists)$ で $\Gamma, \phi(t)$ から $\Gamma, \exists y\, \phi(y)$ が導かれているとき．仮定から $g(m) \models \Gamma(m), \phi(t(m))$ となる g がある．このときは $\max\{g(x), t(x)+1\} \leqq f(x)$ を

みたす f をとれば求める式が得られる．$(\exists <)$ のときも同様．

(5) $(\forall)$ で $\Gamma, \phi(z)$ から$\Gamma, \forall y\, \phi(y)$ が導かれているとき．仮定から $g(m,n) \models \Gamma(m), \phi(n)$ となる g がある．このとき z は下式に現れないので，$(\forall y\, \phi(y))^{\star} = \phi(z)$ として $f = g$ とおけば，求める式が得られる．$(\forall <)$ の場合も同様．

(6) カットで $\Gamma, \neg\phi$ と Δ, ϕ から $\Gamma \cup \Delta$ が導かれているとき．ϕ は Σ_1 だから，特に $\phi(x) = \exists y\, \theta(x,y)$ (θ は有界論理式) としよう．($y = \overrightarrow{y}$ のときも同様に示される．) このとき $\neg\phi(x) = \forall y\, \neg\theta(x,y)$. 仮定から

$$g(m,z) \models \Gamma(m), \neg\theta(m,z), \quad h(m) \models \Delta(m), \exists y\, \theta(m,y) \qquad (*)$$

をみたす単調増加な g, h が存在する．f を関数の合成で定義する．

$$f(x) = g(x, h(x)).$$

いま $f(m) \models \Gamma \cup \Delta(m)$ でないとすると，$f(m) \geq h(m)$ から $h(m) \models \Gamma \cup \Delta(m)$ でないので $(*)$ の右式から，ある $a < h(m)$ で $\theta(m,a)$ が真となる．ところが f の定義から $f(m) > g(m,a)$ だから，同様に $(*)$ の左式で $z = a$ とおけば $\neg\theta(m,a)$ が真となる．これは矛盾である．だから $f(m) \models \Gamma \cup \Delta(m)$ がわかる．

(7) Σ_1 帰納法で Γ, $\phi(0)$ と Γ, $\neg\phi(x)$, $\phi(\mathrm{S}x)$ から $\Gamma, \phi(t)$ が導かれているとき．特に $\phi(x,y) = \exists z\, \theta(x,y,z)$ (θ は有界論理式) としよう．このとき仮定から

$$g(m) \models \Gamma(m), \phi(0,m), \quad h(n,m,z) \models \Gamma(m), \neg\theta(n,m,z), \phi(\mathrm{S}(n),m)$$

をみたす単調増加な g, h がある．f を原始再帰法により定義する．

$$f(0,y) = g(y), \qquad f(x+1,y) = h(x,y,f(x,y)).$$

このとき $f(n,m) \models \Gamma(m), \phi(n,m)$ を n の帰納法で，カット規則のときと同様にして示すことができる．だから，

$$f(t(m),m) \models \Gamma(m), \phi(t(m),m)$$

がわかる．そこで $t(x) \leqq t'(x)$ となる単調増加な原始再帰的関数 t' をとり $f'(x) = f(t'(x),x)$ とおけば，この f' が求めるものとなる．□

この定理 11.4 で $\Gamma = \{\forall \overrightarrow{x}\, \exists y, \phi(\overrightarrow{x}, y)\}$ とおけば，それがパーソンズの定理なので，これでパーソンズの定理が示されたことになる．またこの定理の証明をみ

ると，次のようなたいへん興味ある対応関係もわかる．

証明の推論		関数の生成
Σ_1 カット規則	$\longleftrightarrow$	**関数合成**
Σ_1 帰納法規則	$\longleftrightarrow$	**原始再帰法**

第 12 講　クライゼルの定理 (PA と急増加関数)

12.1　クライゼルの定理の応用

次のクライゼルの定理を使って，ヒドラ-ヘラクレス戦とグッドシュタイン列の命題が PA で証明できないことを示そう．(定理の証明は次節以降で行う．) ここでも簡単のため Σ_1論理式とは $\exists y_1 \cdots \exists y_k\, \theta(\overrightarrow{x}, y_1, \cdots, y_k)$　(θ は有界論理式) のこととしよう．

定理 12.1 **(クライゼル)** $\forall x_1 \cdots \forall x_n\, \exists y\, \phi(x_1, \cdots, x_n, y)$ (ϕ は Σ_1) が PA で証明できるとする．このとき

$$\forall x_1 \cdots \forall x_k\, \exists y < F_\alpha(\max\{x_1, \cdots, x_n\} + 1)\ (\phi(x_1, \cdots, x_n, y))$$

が真となるような急増加関数 F_α ($\alpha < \epsilon_0$) が存在する．

このクライゼルの定理によると，PA で証明できる Π_2文 $\forall \overrightarrow{x}\, \exists y\, \phi(\overrightarrow{x}, y)$ から定義される関数 $f(\overrightarrow{x}) = \mu y(\phi(\overrightarrow{x}, y)$ が真$)$ は急増加関数 F_α で支配される．だから $f \ll F_{\epsilon_0}$ である (図 12.1).

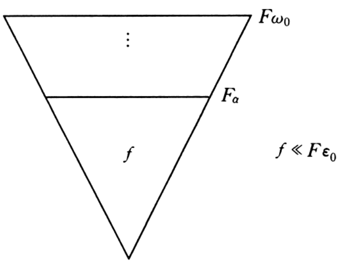


図 12.1

いま命題 10.2「ヘラクレスはヒドラに必ず勝つ」を考えてみよう．この命題は $\forall \alpha\, \exists y\, (\alpha[1][2] \cdots [y] = 0)$ という Π_2文で表現される．これが PA で証明できると

仮定してみよう．そうすると

$$\gamma_m = \omega^{\cdot^{\cdot^{\omega}}} \quad (m \text{ 個の } \omega)$$

を考えたとき，特に $\forall m\,\forall x\,\exists y\,(\gamma_m[x+1][x+2]\cdots[y]=0)$ が証明できるはずである．したがってクライゼルの定理から m, x の関数

$$H_{\gamma_m}(x) = \mu y(\gamma_m[x+1][x+2]\cdots[y]=0)$$

は，ある F_α で支配される．このとき $\alpha < \gamma_{m-1}$ となるような m を固定すれば，$H_{\gamma_m} \ll F_\alpha \ll F_{\gamma_{m-1}}$ である．ところが定理 10.6 から $F_{\gamma_{m-1}} \ll H_{\gamma_m}$ だから矛盾となる．だからこの命題は PA で証明できないことがわかる．

また同様に，命題 10.3「強グッドシュタイン列は 0 に行き着く」が PA で証明できると仮定すると，クライゼルの定理と定理 10.7 から矛盾が導かれるので，これも PA で証明できないことがわかる．以上のことをまとめると，次のようになる．

定理 12.2　(1) 命題 10.2「ヘラクレスはヒドラに必ず勝つ」は PA で証明できない．

(2) 命題 10.3「強グッドシュタイン列は 0 に行き着く」は PA で証明できない．

12.2　PA$^\infty$

クライゼルの定理については，いろいろな証明が知られているが，ここではブッフホルツとウェイナー [1] による方法で示すことにする．

いま，カット消去定理 11.3 の証明で見たように，すべての論理式に対する帰納法規則をもつ PA では，カット消去がうまく行かない．そこで帰納法規則のかわりに，次の (ω) 規則を考えよう．そうすると，カット消去はうまく行くはずである．

$$(\omega)\quad \frac{\Gamma, \phi(0) \quad \Gamma, \phi(\bar{1}) \quad \cdots \quad \Gamma, \phi(\bar{n}) \quad \cdots}{\Gamma, \forall x\, \phi(x)}$$

(これはすべての n に対して $\Gamma, \phi(\bar{n})$ が証明できたとき，$\Gamma, \forall x\, \phi(x)$ が証明できることを表している．)

この考えをもとにして，カット消去がうまく行く体系 PA$^\infty$ を定義していくことにする．

まず最初に前講と同じく，PA を含んでいて，より扱いやすい体系 PA^* を定義しておこう．

定義．(1) PA^* の言語は $=, \neq, 0, \mathrm{S}(x)$ に，原始再帰的関数 f の各定義に対して (こんどは関数記号ではなく) 関係記号 "$f(\overrightarrow{x}) = y$" と，その否定を表す "$f(\overrightarrow{x}) \neq y$" を加えたものとする．
(2) 論理記号は $\vee, \wedge, \exists, \forall$ とする．有界量化記号は入れない．そもそも有界論理式は特殊な原始再帰的関係を表現したものにすぎないので，それに対する関係記号は (1) で与えられていることに注意しよう．その他の記法 (論理式の否定についてや，論理式の集合 Γ を扱うことなど) は前講の $\mathrm{I}^*\Sigma_1$ のときと同じものとする．
(3) PA^* の公理は $\mathrm{I}^*\Sigma_1$ の公理と同じものとする．ただし原始再帰的関数 f の定義式は，対応した関係記号 "$f(\overrightarrow{x}) = y$" についての公理として考えるものとする．たとえば $+$ に対応した述語記号 "$x+y=z$" の公理は以下のものである．($\neg\phi_1, \phi_2$ は実際には $\phi_1 \to \phi_2$ を意味することに再び注意する．)

$t+0=t$

$t+u \neq w,\ t+\mathrm{S}(u) = \mathrm{S}(w)$

$t+u \neq w_1,\ t+u \neq w_2,\ w_1 = w_2$

これらはそれぞれ "$x+0=x$", "$x+\mathrm{S}(y) = \mathrm{S}(x+y)$", "関数値の一意性" を表している．他の関数記号についても同様である．つまり PA^* には関数記号のかわりにまったく同じ働きをする関係記号がある．
(4) 推論規則も $\mathrm{I}^*\Sigma_1$ と同じだが，ただし帰納法規則はすべての論理式 ϕ に適用できるとする．

このように定義された PA^* では，PA の関数記号をそれと同じ働きをする関係記号におきかえて表現できるわけで，PA^* は PA を含んでいることがわかる．

では PA^∞ を以下のように定義しよう．PA^∞ は基本的には PA^* の帰納法規則を上記の (ω) でおきかえたものだが，ただクライゼルの定理を示すためのテクニックとして，新しい述語記号とそれについての公理と推論規則を加えることにする．

定義． (1) PA^∞ の言語は PA^* のものに，新しい 1 変数の述語記号 $x \in N$ とその否定を表す $x \notin N$ を加えたものとする．

(2) PA^∞ の「証明」については次のように考える．

PA^∞ は PA^* の帰納法規則のかわりに，(ω) 規則を入れたものとすると，証明は一般に (これまでの有限の木ではなく) 無限の木の構造をもつ．いまカット消去定理を示すためには，証明の長さ測る必要がある．それをここでは順序数で表すことにする．つまり「長さ α で証明できる」ことを $\vdash^\alpha \Gamma$ と書くことにする．

また PA^∞ の証明に自由変数は必要ないので，証明には文しか現れないし，($\forall$) 規則もないとする．

公理と推論規則は次のものとする．ただし α, β は順序数を表す．

(公理)

$\vdash^\alpha\ \phi$ (ただし ϕ は真な原子式か $0 \in N$)

$\vdash^\alpha\ \bar{n} \in N, \bar{n} \notin N$　(ただし n は任意の自然数)

(推論規則)

($\vee$)　$\vdash^\alpha \Gamma, \phi$　または　$\vdash^\alpha \Gamma, \psi$　ならば　$\vdash^{\alpha+1} \Gamma, \phi \vee \psi$.

($\wedge$)　$\vdash^\alpha \Gamma, \phi$　かつ　$\vdash^\alpha \Gamma, \psi$　ならば　$\vdash^{\alpha+1} \Gamma, \phi \wedge \psi$.

($\exists$)　ある n に対して　$\vdash^\alpha \Gamma, \phi(\bar{n})$　ならば　$\vdash^{\alpha+1} \Gamma, \exists x\, \phi(x)$.

(ω)　すべての n に対して $\vdash^\alpha \Gamma, \phi(\bar{n})$　ならば　$\vdash^{\alpha+1} \Gamma, \forall x\, \phi(x)$.

(カット)　$\vdash^\alpha \Gamma, \neg\phi$　かつ　$\vdash^\alpha \Delta, \phi$　ならば　$\vdash^{\alpha+1} \Gamma \cup \Delta$.

(このとき，ϕ はカット論理式と呼ばれる．)

(増)　$\vdash^\alpha \Gamma$　かつ　$\Gamma \subseteq \Delta$　ならば　$\vdash^\alpha \Delta$.

(N)　$\vdash^\alpha \Gamma,\ \bar{n} \in N$　ならば　$\vdash^{\alpha+1} \Gamma,\ \mathrm{S}(\bar{n}) \in N$.

(累積)　$\vdash^\alpha \Gamma$　かつ　$\alpha <_k \beta$　ならば　$\vdash^\beta \Gamma$.

ただし，$k = \max\{3, 3n \mid \bar{n} \notin N$ が Γ に入る $\}$ とする．

また $\alpha <_k \beta$ の定義については定理 10.4 の 2 を参照のこと．このとき定理 10.4 の 3 より，$F_\alpha(x) \leq F_\beta(x)$ $(x \geq k)$ が成り立つことに注意する．

さて，このよう定義された PA^∞ には，PA^* が次の定理の「埋め込み」の意味で，含まれていることがわかる．

定理 12.3 (埋め込み定理) $\Gamma(\overrightarrow{x})$ が PA* で証明できるとする．このときある順序数 $\alpha = \omega \cdot b$ ($b < \omega$) が存在して，すべての $\overrightarrow{n} = \overline{n_1}, \cdots, \overline{n_r}$ に対して

$$\vdash^{\alpha} \ \overline{n_1} \notin N, \cdots, \overline{n_r} \notin N, \ \Gamma^N(\overrightarrow{n}).$$

ただし $\Gamma^N(\overrightarrow{n})$ は Γ 内の $\forall y(\cdots)$ と $\exists y(\cdots)$ をそれぞれ $\forall y(y \notin N \vee \cdots)$ と $\exists y(y \in N \wedge \cdots)$ ですべておきかえ，$\overrightarrow{x}$ を $\overrightarrow{n}$ でおきかえたものとする．

[証明] PA* の証明の長さ (使われた推論規則の数) の帰納法で示そう．まず，Γ が PA* の公理のときは，Γ に論理記号は含まれないし，$\Gamma(\overrightarrow{n})$ には真な原始式が必ず含まれるので，この定理の主張がわかる．

次に Γ が PA* の推論規則で導かれたとき．ここでは帰納法規則のときのみ示そう．(他の場合も同様にできる．) 簡単のため $\Gamma^N = \Gamma$, $\phi^N = \phi$ とする．いま帰納法の仮定から $\alpha = \omega \cdot b$ に対し，

$$\vdash^{\alpha} \ \Gamma, \phi(0). \quad \vdash^{\alpha} \ \bar{n} \notin N, \Gamma, \neg\phi(\bar{n}), \phi(\mathrm{S}(\bar{n})).$$

一方 $\vdash^{\alpha+n+1} 0 \in N$ から (N) を繰り返して $\vdash^{\alpha+2n+1} \bar{n} \in N$ となる．だから，$\vdash^{\alpha} \Gamma, \phi(0)$ から始めて，次のようにカットを繰り返すと，

$$\vdots$$

$$(\text{カット}) \ \dfrac{\vdash^{\alpha+2n} \Gamma, \phi(\bar{n}) \qquad \vdash^{\alpha} \bar{n} \notin N, \Gamma, \neg\phi(\bar{n}), \phi(\mathrm{S}(\bar{n}))}{(\text{カット}) \ \dfrac{\vdash^{\alpha+2n+1} \bar{n} \notin N, \Gamma, \phi(\mathrm{S}(\bar{n})) \qquad \vdash^{\alpha+2n+1} \bar{n} \in N}{\vdash^{\alpha+2n+2} \Gamma, \phi(\mathrm{S}(\bar{n}))}}$$

結局すべての n について，$\vdash^{\alpha+2n} \Gamma, \phi(\bar{n})$ となる．(増) と (累積) から，$\vdash^{\alpha+\omega} \bar{n} \notin N, \Gamma, \phi(\bar{n})$ だから $(\vee)$ と (ω) により

$$\vdash^{\alpha+\omega+2} \ \Gamma, \forall x(x \notin N \vee \phi(x)).$$

$\alpha = \omega \cdot b$ より $\alpha + \omega + 2 <_k \omega \cdot (b+2)$ だから，定理の主張が帰納法規則の適用に関しても保たれることがわかった．したがって定理が成り立つ．□

この定理の証明からは，PA* の証明に対応して存在する PA^{∞} の証明のカット論理式の長さ (含まれる論理記号の数) は，元の PA* の証明に現れる論理式の長さを越えないこともわかる．

12.3　カット消去定理

PA^{∞} には帰納法規則がないので，論理記号を含むカット論理式をもつカットは消去できる．しかし前講のカット消去定理で見たように，カットを消去すると一般に証明は長くなってしまう．いま，証明の長さは順序数であったので，カットを消去したとき証明の長さがどのように変化するかを見て行こう．

いま長さ α の Γ の証明があって (つまり $\vdash^{\alpha}\ \Gamma$), その証明の各カット論理式の長さ (含まれる論理記号の数) が $\leqq r$ であるとき，Γ はカットランク$\leqq r$ で証明できるといい，$\vdash^{\alpha}_{r}\ \Gamma$ と書くことにする．このとき次の補題が成り立つ．

補題 12.4　長さ $r+1$ の論理式 ϕ に対して，$\vdash^{\alpha}_{r} \Gamma, \neg\phi$ かつ $\vdash^{\beta}_{r} \Delta, \phi$ とする．このとき，$\vdash^{\alpha\#\beta}_{r}\ \Gamma \cup \Delta$ である．

ただし $\alpha\#\beta$ は順序数の自然和で次のように定義されたものである．

$$\alpha = \omega^{\alpha_1} + \cdots + \omega^{\alpha_n}, \quad \beta = \omega^{\beta_1} + \cdots + \omega^{\beta_m}$$

の指数部 α_i, β_j を大きさ順に並びかえて $\delta_1 \geqq \cdots \geqq \delta_{n+m}$ とおいたとき

$$\alpha\#\beta = \omega^{\delta_1} + \cdots + \omega^{\delta_{n+m}}.$$

この補題は $\alpha\#\beta$ の超限帰納法によって証明できるが，その証明はここでは省略する．次にこれを使ってカット消去定理を示そう．

定理 12.5 (カット消去定理) $\vdash^{\alpha}_{r+1} \Gamma$ のとき，$\vdash^{\omega^{\alpha}}_{r} \Gamma$ となる．

だからこの定理を繰り返すと $\vdash^{\alpha^*}_{0} \Gamma$ ($\alpha^* = \omega^{\cdot^{\cdot^{\omega^{\alpha}}}}$ (r個のω)) となる (図 12.2).

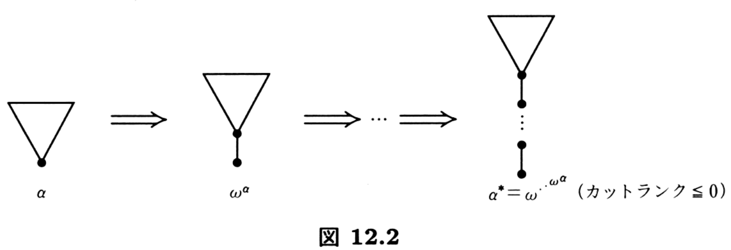


図 12.2

[証明]　α の超限帰納法によって示そう．ここでは特にカットにより $\vdash^{\alpha}_{r+1} \Gamma, \neg\phi$

と $\vdash^{\alpha}_{r+1}\ \Delta,\phi$ から $\vdash^{\alpha+1}_{r+1}\ \Gamma\cup\Delta$ を導く場合のみを扱おう．いま帰納法の仮定から $\vdash^{\omega^\alpha}_{r}\ \Gamma,\neg\phi$ かつ $\vdash^{\omega^\alpha}_{r}\ \Delta,\phi$ だから上の補題より $\vdash^{\omega^\alpha+\omega^\alpha}_{r}\ \Gamma\cup\Delta$. このとき

$$\omega^\alpha+\omega^\alpha <_k \omega^\alpha\cdot(k+1)=\omega^{\alpha+1}[k] <_k \omega^{\alpha+1}$$

だから (累積) より $\vdash^{\omega^{\alpha+1}}_{r}\ \Gamma\cup\Delta$ なので定理が示された．□

12.4　クライゼルの定理の証明

まず次の補題を示してからクライゼルの定理を証明しよう．

いま論理式が $\Sigma_1(N)^+$ であるとは，原子式と $x\in N$ から $\vee,\wedge,\exists$ のみを使ってできたもので，自由変数は含まないものと定義する．$\Sigma_1(N)^+$ 論理式の有限集合 Γ と自然数 n に対して，

$$n\models\Gamma$$

とは，N を集合 $\{i\mid i<n\}$ と解釈したとき，ある $\phi_j\in\Gamma$ が真のときとする．このとき次の補題が成り立つ．

補題 12.6　Γ を $\Sigma_1(N)^+$ 論理式の集合とし，$\vdash^{\alpha}_{0}\ \overline{n_1}\notin N,\cdots,\overline{n_m}\notin N,\Gamma$ とする．このとき $F_\alpha(k)\models\Gamma$ が成り立つ．ただし $k=\max\{3,3n_1,\cdots,3n_m\}$.

[証明]　α に関する超限帰納法によって示そう．簡単のため $m=1$ としよう．まず，与式が公理のとき．公理が真な論理式を含むときは明らかに成り立つ．公理が $0\in N$ を含むときは，$0<F_\alpha(k)$ だから成り立つ．公理が $\vdash^{\alpha}\ \bar{n}\notin N,\bar{n}\in N$ のときは，$k=\max\{3,3n\}$ だから $n<F_\alpha(k)$ となるので成り立つ．

次に推論規則により与式が導かれている場合を考えよう．いま Γ は $\forall$ を含まないので (ω) は考えなくてよいことに注意する．ここでは推論規則がカットの場合のみを示そう．他の場合は容易に示される．つまり，カットで (i) $\vdash^{\alpha}_{0}\ \bar{n}\notin N,\Gamma,\neg\phi$ と (ii) $\vdash^{\alpha}_{0}\ \bar{n}\notin N,\Delta,\phi$ から $\vdash^{\alpha+1}_{0}\ \bar{n}\notin N,\Gamma\cup\Delta$ が導かれているときとしよう．

もし ϕ が $\bar{m}\in N$ の形でなければ ϕ か $\neg\phi$ が偽なので，帰納法の仮定から求める式 $F_{\alpha+1}(k)\models\Gamma\cup\Delta$ が得られる．

もし ϕ が $\bar{m}\in N$ の形ならば，(ii) の帰納法の仮定から $F_\alpha(k)\models\Delta$ または

$F_\alpha(k) \models \bar{m} \in N$. 前者の場合は求める式がすぐにわかる．後者の場合はすなわち $m < F_\alpha(k)$ のことだから，

$$F_\alpha(\max\{k, 3m\}) \leqq F_\alpha(3F_\alpha(k)) \leqq F_\alpha^3(k) \leqq F_{\alpha+1}(k)$$

となる．(i) の帰納法の仮定は $F_\alpha(\max\{k, 3m\}) \models \Gamma$ だから求める式が得られる．

□

さてクライゼルの定理 12.1 の証明を考えよう．クライゼルの定理の $\phi(\overrightarrow{x}, y)$ は Σ_1 なので，$\forall \overrightarrow{x}\ \exists y\ \phi(\overrightarrow{x}, y)$ は $\forall \overrightarrow{x}\ \exists y\ \exists \overrightarrow{z}\ \theta(\overrightarrow{x}, y, \overrightarrow{z})$ (θ は有界論理式) と書ける．また並んだ $\exists$ は 1 つの $\exists$ にまとめることができる．たとえば，

$$\exists y\ \exists z\ \theta(y, z) \longleftrightarrow \exists w\ \theta((w)_0, (w)_1)$$

と $(w)_0 \leqq w$ と $(w)_1 \leqq w$ が PA で証明できるのでよい．また PA は PA* に含まれるが，そのとき PA の有界論理式は PA* では，それを表現する原始再帰的関係に対する関係記号で置きかわっていることに注意しよう．以上のことから，クライゼルの定理は次を示せば十分であることがわかる．

定理 12.7 (クライゼル) $\forall \overrightarrow{x}\ \exists y\ \theta(\overrightarrow{x}, y)$　(θ は PA* の関係記号) が PA* で証明できるとし，関数 f を

$$f(\overrightarrow{x}) = \mu y(\theta(\overrightarrow{x}, y) \text{ が真})$$

と定義する．このとき $f(\overrightarrow{x}) < F_\alpha(\max\{1, \overrightarrow{x}\})$ となる $\alpha < \epsilon_0$ が存在する．

[証明]　埋め込み定理 12.3 から $\alpha = \omega \cdot b\ (b < \omega)$ と $r < \omega$ に対し

$$\vdash_r^\alpha\ \overline{n_1} \notin N, \cdots, \overline{n_r} \notin N, \exists y\,(y \in N \wedge \theta(\overrightarrow{n}, y)).$$

がすべての $\overrightarrow{n} = \overline{n_1}, \cdots, \overline{n_r}$ で成り立つ．このこととカット消去定理 12.5 から，

$$\vdash_0^{\alpha^*}\ \bar{n_1} \notin N, \cdots, \bar{n_r} \notin N, \exists y\,(y \in N \wedge \theta(\overrightarrow{n}, y)).$$

だから上の補題 12.6 より $F_{\alpha^*}(\max\{3, 3\overrightarrow{n}\}) \models \exists y\ \theta(\overrightarrow{n}, y)$ が成り立つ．すなわち $f(\overrightarrow{n}) < F_{\alpha^*}(\max\{3, 3\overrightarrow{n}\})$．いま，$F_{\alpha^*}(\max\{3, 3\overrightarrow{n}\}) \leqq F_{\alpha^*+1}(\max\{1, \overrightarrow{n}\})$ は容易にわかるから，

$$f(\overrightarrow{n}) < F_{\alpha^*+1}(\max\{1, \overrightarrow{n}\})$$

が成り立つ．だから定理の α として $\alpha^* + 1$ をとればよい．□

クライゼルの定理はPAでの独立性を示すときに利用されるだけでなく，PAで証明できる Π_2文から定まる関数 $f(\overrightarrow{x})$ の「複雑さ」を示した内容になっている点でたいへん興味深い．

第13講 パリス-ハーリントンの独立命題

13.1 パリス-ハーリントンの命題 PH

この講ではパリス-ハーリントンの組合せ的命題 PH は，真ではあるが PA で証明できないことを示そう．

PH はグラフ理論のラムゼイ性についての命題である．ラムゼイ性とは「集合 X が十分大きければ，ある種の等質性をもった大きな部分集合 Y が存在する」という現象を意味していて，たとえば「3人いれば2人は同性」とか,「6人いればある3人は互いに知り合いか，まったく知り合いでない (図 13.1)」とか,「r 個の引き出しに $r+1$ 個の玉を入れると，どこかの引き出しには2個以上の玉が入る」といった性質である．ラムゼイ性は数学のいろいろな局面で現れるので，PH は「実際の数学での独立命題」と呼ぶにふさわしいものとなっている．

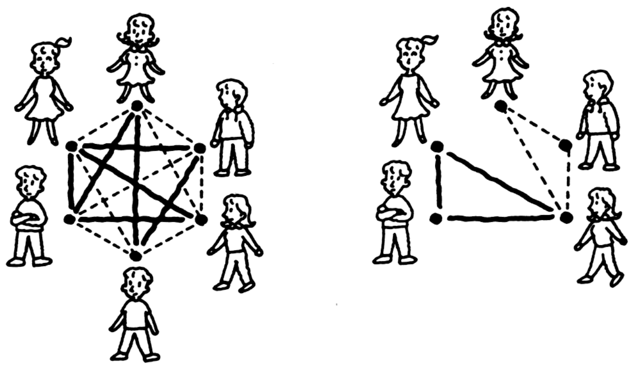


図 13.1

まず組合せ論やグラフ理論で有名な，有限ラムゼイの定理を述べよう．自然数 $x \leqq y$ に対して，$[x,\ y]$ は通常の区間 $\{x, x+1, \cdots, y\}$ を表すとする．また $^{\#}X$ を集合 X の元の個数とし，

$$[X]^n = \{Y \subseteqq X \mid {}^{\#}Y = n\} \ (n \text{ 個の } X \text{ の元の組全体})$$

とする．簡単のために自然数 r は区間 $[0,\ r-1]$ と同一視する．いま，関数 f :

$[X]^n \to r\ (= [0,\ r-1])$ に対して集合 $Y(\subseteqq X)$ が f-等質であるとは，$f : [Y]^n \to r$ が一定の値をとるときをいう．

有限ラムゼイの定理 $n, r, x > 0$ に対し y が存在して，$X = [0,\ y]$ とおくと，すべての $f : [X]^n \to r$ に対し，次の (1), (2), (3) をみたす $Y(\subseteqq X)$ がある．

(1) Y は f-等質である，

(2) $^{\#}Y \geqq n+1$,

(3) $^{\#}Y \geqq x$.

たとえば，上記の「3 人いれば 2 人は同性」は，有限ラムゼイの定理で $n=1$, $r=2$, $x=2$ のとき $y=3$ とすればよい．「6 人いればある 3 人は互いに知り合いか，まったく知り合いでない」は $n=2$, $r=2$, $x=3$ のとき $y=6$ とすればよい．この定理をほんの少し変形したものが次の PH である．

命題 PH (パリス-ハーリントン) $n, r, x > 0$ に対し y が存在して，$X = [x,\ y]$ とおくと，

- すべての $f : [X]^n \to r$ に対し次の (1), (2), (3) をみたす $Y(\subseteqq X)$ がある．
  (1) Y は f-等質である，
  (2) $^{\#}Y \geqq n+1$,
  (3) $^{\#}Y \geqq \min(Y)$.

PH と有限ラムゼイの定理との違いは条件 (3) が本質的である．$\min(Y) \geqq x$ だから PH から有限ラムゼイの定理はすぐ導かれる．実際には PH は PA で証明できないのに対し，有限ラムゼイの定理は $I\Sigma_1$ で証明できることが知られている．

さて，いま PH の • 以下の部分を $X \longrightarrow (*)^n_r$ と表すことにしよう．これは n, r, x, y について原始再帰的な関係である．このとき PH は次の Π_2文で表される．

$$\mathrm{PH} \equiv \forall n\, \forall r\, \forall x\, \exists y\, ([x, y] \longrightarrow (*)^n_r).$$

次の節では PH は真であることが示される．だから関数 $g(n, r, x)$ を PH をみたす

最小の y として定義できる．

$$g(n,r,x)=\mu y([x,y]\longrightarrow(*)^n_r \text{ が真}).$$

これから示したいことは，この関数 g がどの急増加関数 F_α でも支配されない，ということである．それが示されれば，ヒドラ-ヘラクレス戦の命題やグッドシュタイン列の命題と同じように，PH が PA で証明できないことがわかる．

13.2　PH が真であること

ここで PH が真であることを示そう．そのために PH が真でないと仮定してみよう．つまりある n, r, x があって任意の $X=[x,\ y]$ に対して，ある $f:[X]^n\to r$ が存在し,「f-等質かつ $^\#Y\geq n+1$ である任意の $Y(\subsetneqq X)$ に対して $^\#Y<\min(Y)$ となる」．

この「　」をみたすような f のことを**反例**と呼ぼう．いま n, r, x は固定されて y は自然数を動くとする．反例 f, f' に対し

$$f\preceq f'\iff f \text{ は } f' \text{ の制限}$$

$$(\mathrm{dom}\,(f)\subsetneqq\mathrm{dom}\,(f') \text{ かつ } \mathrm{dom}\,(f) \text{ 上で両関数は一致})$$

で順序を定義すると，反例全体は (y が自然数を動くので無限の) 木と考えることができる．この木の各点における枝分かれは高々 r 本しかないので有限である．そこでケーニッヒの補題 (下の注を参照) より，この無限の木はある無限の道

$$f_0\preceq f_1\preceq f_2\preceq\cdots$$

をもつ．この無限の道の意味するところはすなわち，ある $f:[\{x,x+1,\ \cdots\}]^n\to r$ があって，任意の $X=[x,\ y]$ に対して $f:[X]^n\to r$ が反例となることである．このとき無限ラムゼイの定理 (下の注を参照) をこの f に対して適用すると，ある無限集合 $Y\subsetneqq\{x,x+1,\cdots\}$ で f-等質なものが存在する．

いま X を (すなわち y を) 十分大きくとると $^\#(Y\cap X)\geq\min(Y\cap X)$ となるが，これは $f:[X]^n\to r$ が反例であることに矛盾する．これで PH が真であることが示されたことになる．　□

注．上の証明に使われた 2 つの定理を証明なしで述べておこう．

ケーニッヒの補題 各点で有限の枝分かれしかしない無限の木は，ある無限の道(全順序部分集合) をもつ．

無限ラムゼイの定理 $f:[X]^n \to r$ (X は無限集合) に対して，f-等質な無限集合 $Y(\subsetneqq X)$ が必ず存在する．

これらはどちらも無限集合についての命題 (2 階算術の命題) なので，1 階算術である PA での独立性の証明に直接には関係してこない．しかし，PH は無限ラムゼイの定理を「有限化」して得られるということから，これらの命題の 2 階算術の枠組みでの研究は，たいへん重要なものなのである．(補講の「逆数学プログラム」を参照のこと．)

13.3 PH(2) が $I\Sigma_1$ で証明できないこと

PH で特に $n=2$ とおいた次の命題が $I\Sigma_1$ で証明できないことを示そう．

$$\mathrm{PH}(2) \equiv \forall r \forall x \exists y \, ([x,y] \longrightarrow (*)^2_r).$$

アイデアは，PH の $f:[X]^2 \to r$ を $C:[\omega]^2 \to r$ に拡張して考えることにある．ただし ω は $\{n \mid n<\omega\}$ (自然数全体) と同一視する．このとき $C:[\omega]^2 \to r$ が関数 $F:\omega \to \omega$ を捕らえるとは，C-等質な Y で $^{\#}Y \geqq 3$, $^{\#}Y \geqq \min(Y)$ であるものは必ず，

$$\text{(i)}\ \min(Y) \geqq 3, \qquad \text{(ii)}\ x,y \in Y,\ x<y \text{ ならば } F(x) \leqq y$$

となることをいう．このとき次の補題から PH(2) は $I\Sigma_1$ で証明できないことがわかる．

補題 13.1 急増加関数 F_m $(m<\omega)$ を捕らえる $C_m:[\omega]^2 \to 4\cdot 3^m$ がある．

[証明] m の帰納法で示そう．いま $x<y$ のとき $C(\{x,y\})$ を単に $C(x,y)$ と書く．また集合 $\{y_1,\cdots,y_k\}$ も $y_1<\cdots<y_k$ のとき $\{y_1<\cdots<y_k\}$ と書くことに

する．$C_0 : [\omega]^2 \to 4$ を次のように定義しよう．

$$C_0(x, y) = \begin{cases} 0, & x = 0 \\ 1, & x = 1 \\ 2, & x = 2 \\ 3, & x \geqq 3 \end{cases}$$

C_0 が F_0 を捕らえることを示そう．$Y = \{y_1 < \cdots < y_k\} (k \geqq 3)$ を C_0-等質とすると，$y_1 \neq y_2$ から $C_0(y_1, y_2) = C_0(y_2, y_3)$ の値は 0, 1, 2 ではない．だから (i) $y_1 \geqq 3$. また $F_0(x) = x + 1$ から (ii) が成り立つので C_0 は F_0 を捕らえることがわかる．

次に C_m の存在を仮定し $C_{m+1} : [\omega]^2 \to 4 \cdot 3^{m+1}$ を次で定義する．

$$C_{m+1}(x, y) = \begin{cases} 3 \cdot C_m(x, y), & y < F_m^{x-1}(x) \\ 3 \cdot C_m(x, y) + 1, & F_m^{x-1}(x) \leqq y < F_{m+1}(x) \\ 3 \cdot C_m(x, y) + 2, & F_{m+1}(x) \leqq y \end{cases}$$

C_{m+1} が F_{m+1} を捕らえることを示そう．いま C_{m+1}-等質な

$$Y = \{y_1 < \cdots < y_k\} \ (k \geqq 3; \ \ k \geqq y_1)$$

に対して，C_{m+1} の定義から Y は C_m-等質でもある．C_m は F_m を捕らえるから (i) $y_1 \geqq 3$ であり，その (ii) と $k \geqq y_1$ から

$$y_k \geqq F_m(y_{k-1}) \geqq \cdots \geqq F_m^{k-1}(y_1) \geqq F_m^{y_1 - 1}(y_1).$$

だから $C_{m+1}(y_1, y_k)$ は $3 \cdot a$ の形ではない．それゆえ Y の等質性から，すべての i に対して $y_{i+1} \geqq F_m^{y_i - 1}(y_i)$ となるので，

$$y_3 \geqq F_m^{y_2 - 1}(y_2) \geqq F_m^{2y_1 - 2}(y_1) \geqq F_m^{y_1 + 1}(y_1) = F_{m+1}(y_1).$$

つまり $C_{m+1}(y_1, y_3)$ は $3 \cdot a + 2$ の形である．Y の等質性から (ii) $F_{m+1}(y_i) \leqq y_{i+1}$ となるので，C_{m+1} は F_{m+1} を捕らえることがわかる．□

この C_m を使えば次のように PH(2) は $\mathrm{I}\Sigma_1$ で証明できないことがわかる．$r = 4 \cdot 3^m$ としよう．いま $g(2, r, x) = y$ とおくと，y は PH$(n = 2)$ を成り立たせるから，$C_m : [x, y]^2 \to r$ に対して C_m-等質なある $Y = \{y_1 < \cdots < y_k\} (k \geqq 3)$ が存在して $^{\#}Y \geqq \min(Y)$ となる．C_m は F_m を捕らえるから

$$F_m(x) \leqq F_m(y_1) \leqq y_2 < y_3 \leqq y = g(2,\ 4 \cdot 3^m, x). \qquad (*)$$

一方，もし PH(2) が $I\Sigma_1$ で証明できるとすると，パーソンズの定理 11.1 から r, x の関数 $g(2, r, x)$ はある F_m で支配されるが，$r = 4 \cdot 3^m$ とおき $x(\geqq r)$ を十分大きくとれば式 $(*)$ に矛盾する．だから次の定理が証明できたことになる (図 13.2).

定理 13.2 PH(2) は $I\Sigma_1$ で証明できない．

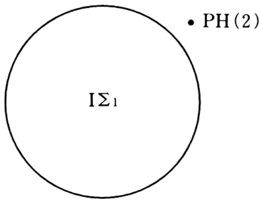


図 13.2

13.4 PH が PA で証明できないこと

PH が PA では証明できないことを示そう．ここではレーブルとネストリル [2] の方法による．アイデアは，PH の $f : [X]^n \to r$ を順序数 α に対する $f : [\alpha]^n \to r$ に拡張することにある．ただし α は集合 $\{\beta \mid \beta < \alpha\}$ (α より小さい順序数全体) と同一視する．

いま 13.2 節で考えた「反例」の順序数への拡張版となる「パリス色付け」を定義しよう．つまり，関数 $f : [\alpha]^n \to r$ が (n, r) パリス色付けであるとは，f-等質な $Y(\subsetneqq \alpha)$ で ${}^{\#}Y \geqq n + 1$ なものは，

$${}^{\#}Y \leq h(\max Y) + c(\max Y)$$

をみたすときとする．ただし h と c は次のように定義される．

(1) $h(\alpha)$ は α の高さを表す．つまり $\alpha < \omega^{\cdot^{\cdot^{\omega}}}$ (h 個のω) をみたす最小の $h > 0$ のこと．

(2) $c(\alpha)$ は α に現れる順序数の表現の長さと係数の最大値を表す．つまり次のように再帰的に定義される．

(2a)　$c(0) = 0$.

(2b)　$\alpha = \omega^{\alpha_1} \cdot n_1 + \cdots + \omega^{\alpha_k} \cdot n_k (\alpha_1 > \cdots > \alpha_k)$ に対して，

$$c(\alpha) = \max\{k, n_1, \cdots, n_k, c(\alpha_1), \cdots, c(\alpha_k)\}.$$

このとき基本列の定義を考えてみると次の性質がわかる．

性質　$c(\alpha) \leqq x$ ならば $c(\alpha[x]) \leqq x + 1$.

さてクライゼルの定理から PH の独立性を示すことを考えよう．いま最終的に求めたいのは，PH をみたす最小の y を与える関数 $g(n, r, x)$ がどの急増加関数でも支配されない，という事実である．そこで次の 2 つの補題を準備しよう．まず 1 つめはパリス色付けの存在を「仮定」して，g がどの急増加関数でも支配されないことを述べたものである．パリス色付けの「存在」は 2 つめの補題で示そう．

補題 13.3　パリス色付け $f : [\alpha]^n \to r$ が存在するとき，

$$H_\alpha(x) + q < g(n, r, x + 1 + q) \quad (c(\alpha) \leqq x + 1 \text{ に対して})$$

が成り立つ．ただし $q = h(\alpha) + 2$.

[証明]　g の定義 (13.1 節) から，この不等式を示すためには 13.2 節の「反例」

$$f' : [(x + 1) + q,\ y + q]^n \to r \qquad (y = H_\alpha(x))$$

を作ればよいことは容易にわかる．いま x を固定して自然数の上昇列

$$X = \{(x + i) + q \mid i = 1, 2, \cdots\}$$

を考えたとき，関数 $O : X \to \alpha$ を次のように定義しよう．

$O((x + 1) + q) = \alpha[x + 1]$,

$O((x + 2) + q) = \alpha[x + 1][x + 2]$,

$\cdots$ 一般に $O((x + i) + q) = \alpha[x + 1][x + 2] \cdots [x + i]$.

これは順序数の下降列をなし，$O(y + q) = 0$ となる最小の y がまさに $H_\alpha(x)$ であった (10.3 節). そこで $f' : [(x+1)+q,\ y+q]^n \to r$ を次のように定義しよう．

$$f'(z_1, \cdots, z_n) = f(O(z_1), \cdots, O(z_n)).$$

このとき f' は反例となる．なぜなら f'-等質な $Y = \{y_1 + q < \cdots < y_m + q\} (m \geqq n + 1)$ に対し，$O(Y)$ は f-等質で f がパリス色付けだから

$$^{\#}Y = {}^{\#}O(Y) \leqq c(\max O(Y)) + h(\max O(Y)).$$

ここで $\max O(Y)$ は O の定義より $\alpha[x+1][x+2]\cdots[y_1]$ である．

一方 $c(\alpha) \leqq x+1$ と上の性質を繰り返し適用することにより

$$c(\alpha[x+1][x+2]\cdots[y_1]) \leqq y_1+1$$

がわかるので，結局

$$^{\#}Y \leqq (y_1+1)+h(\max O(Y)) < y_1+q.$$

だから f' は反例である．これで補題が示されたことになる．□

この補題により，パリス色付けの存在を仮定すれば「反例」が導かれることがわかったので，次の補題でそのパリス色付けの「存在」を示そう．

補題 13.4 高さ $h \geqq 2$ の順序数に対する $(h+1, 3^{(h-1)^2})$ パリス色付け f_h が存在する．

[証明] h の帰納法による．まず $h=2$ のときを示そう．順序数 $\alpha>0$ を

$$\alpha=\omega^{\alpha_1}\cdot n_1+\cdots+\omega^{\alpha_t}\cdot n_t \ (\alpha_1>\cdots>\alpha_t)$$

と表したとき，n_i を ω^{α_i} の係数，α_i を指数部とよぶ．ω^σ の係数を $co(\alpha,\sigma)$ と書く．(ω^σ が α 内になければ $co(\alpha,\sigma)=0$ とする．) $\alpha>\beta$ に対して

$$\overline{\alpha\beta}=\max\{\,\sigma \mid co(\alpha,\sigma)\neq co(\beta,\sigma)\}$$

と定義する．これは異なる係数をもつものの指数部で最大のものを表している．このとき $P:[\epsilon_0]^3 \to 3$ を次で定義する．

$$P(\{\alpha>\beta>\gamma\})=\begin{cases}0, & \overline{\alpha\beta}>\overline{\beta\gamma}\\ 1, & \overline{\alpha\beta}=\overline{\beta\gamma}\\ 2, & \overline{\alpha\beta}<\overline{\beta\gamma}\end{cases}$$

$P:[\omega^\omega]^3 \to 3$ が (3,3) パリス色付けであることを示そう．いま P-等質な $Y=\{\delta_1>\cdots>\delta_k\}(k\geqq 4)$ に対して次の性質がある．($\sigma_i=\overline{\delta_i\delta_{i+1}}$ とおく．)

(1) $P(Y)=1$ のとき $k \leqq c(\delta_1)+1$.

[(1) の証明] このとき P の定義から$\sigma_i(=\sigma)$ は i に依らず一定だから，ω^σ の係数の方が下降列をなすはず．

$$co(\delta_1,\sigma)>co(\delta_2,\sigma)>\cdots>co(\delta_k,\sigma).$$

この式と c の定義から $k-1 \leqq co(\delta_1, \sigma) \leqq c(\delta_1)$ だから求める式が得られる．

(2) $P(Y) = 2$ のとき $k \leqq c(\delta_1) + 1$.

[(2) の証明]　このとき P の定義から $\sigma_1 < \sigma_2 < \cdots < \sigma_{k-1}$ となるので，δ_1 の指数部にすべての σ_i が現れることがわかる．たとえば

$$\sigma_2 > \sigma_1 = \max\{\sigma \mid co(\delta_1, \sigma) \neq co(\delta_2, \sigma)\}$$

なので，$co(\delta_1, \sigma_2) = co(\delta_2, \sigma_2)$ のはず．だから δ_1 の指数部には σ_2 が現れる $\cdots$ など．よって $c(\delta_1) \geqq k-1$ だから求める式が得られる．

(3) $P(Y) = 0,\ \delta_1 < \omega^\omega$ のとき $k \leqq c(\delta_1) + 2$.

[(3) の証明]　このとき P の定義から $\omega > \sigma_1 > \sigma_2 > \cdots > \sigma_{k-1}$ となるので，この式と c の定義から $k-2 \leqq \sigma_1 \leqq c(\delta_1)$ だから求める式が得られる．

これら (1), (2), (3) のいずれの場合でも，$\delta_1 < \omega^\omega$ のとき

$${}^{\#}Y = k \leqq c(\delta_1) + h(\delta_1) \quad (\delta_1 = \max Y)$$

が成り立つので $P : [\omega^\omega]^3 \to 3$ は (3,3) パリス色付けである．

次に f_{h-1} を使って $f_h : [\gamma_h]^{h+1} \to 3^{(h-1)^2}$ を定義しよう．上の $P : [\epsilon_0]^3 \to 3$ を使う．いま $X = \{\delta_1 > \cdots > \delta_{h+1}\}$, $P_i = P(\delta_i, \delta_{i+1}, \delta_{i+2})$ とおく．

(i) $P_1 = \cdots = P_{h-1} = 0$ のとき．上の (3) と同様に $\sigma_1 > \cdots > \sigma_h$ なので，

$$f_h(X) = f_{h-1}(\sigma_1, \cdots, \sigma_h)$$

と定義する．(このとき帰納法の仮定から $f_h(X) < 3^{(h-2)^2}$ となっている．)

(ii) $P_1 = \cdots = P_{h-1} = 0$ でないとき．

$$f_h(X) = (P_1, \cdots, P_{h-2}\ ;\ P_2, \cdots, P_{h-1})$$

と定義する．ただし実際にはこのベクトル値は，とりうる値の個数が $\leqq 3^{h-1}$ だから，(i) の範囲より外の $3^{(h-2)^2}$ から $3^{(h-2)^2} + 3^{h-1} \leqq 3^{(h-1)^2}$ までの適当な自然数値をとると考えてよい．

この f_h がパリス色付けであることを示そう．いま f_h-等質な

$$Y = \{\delta_1 > \delta_2 > \cdots > \delta_k\} \quad (k \geqq h+2)$$

に対して，$f_h(Y)$ の値は次の 2 つの場合が考えられる．まずその値が (i) で定義される場合は，集合 $\{\sigma_1 > \cdots > \sigma_{k-1}\}$ は f_{h-1}-等質であり，f_{h-1} は

パリス色付けより，

$$k-1={}^{\#}Y-1 \leqq c(\sigma_1)+h(\sigma_1).$$

ここで c, h の定義より $c(\sigma_1) \leqq c(\delta_1)$ と $h(\sigma_1)=h(\delta_1)-1$ が成り立つので，

$${}^{\#}Y \leqq c(\delta_1)+h(\delta_1)=c(\max(Y))+h(\max(Y)).$$

次に $f_h(Y)$ の値が (ii) で定義される場合は Y が f_h-等質より，

$$(P_1,\cdots;P_2,\cdots)=(P_2,\cdots;P_3,\cdots)=\cdots=(P_{k-h},\cdots;P_{k-h+1},\cdots)$$

なので $P_1=P_2=\cdots=P_{k-2}$ がわかる．いまこれが $=0$ ではない場合だから $=1$ か $=2$ である．このとき上の (1),(2) と同様に次が成り立つ．

$${}^{\#}Y \leqq c(\delta_1)+1 \leqq c(\max(Y))+h(\max(Y)).$$

結局，どちらの場合も f_h がパリス色付けの条件をみたすことが示された．

□

さて定理 10.6 と上の 2 つの補題からただちに，$c(\omega^\alpha) \leqq x+1$ に対して

$$F_\alpha(x) \leqq H_{\omega^\alpha}(x) < g(h+1,\ r,\ x+h+3)$$

が得られる．ただし $h=h(\omega^\alpha)$, $r=3^{(h-1)^2}$. このときもし PH が PA で証明できると仮定すると，クライゼルの定理 12.1 より，$g(h+1,r,x+h+3)$ はある急増加関数 F_α によって支配されるが，それはこの不等式に矛盾する．だから PH が PA で証明できないことがわかる．

なお，実際には $n<\omega$ を固定したときの

$$\mathrm{PH}(n) \equiv \forall r\,\forall x\,\exists y\,([x,y] \longrightarrow (*)^n_r)$$

は PA で証明できることが知られている．以上のことを定理として述べておこう (図 13.3).

定理 13.5 PH は PA で証明できない．(PH(n) は PA で証明できる．)

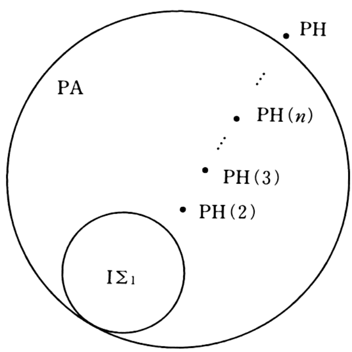


図 13.3

パート C 参考文献

パート C では以下の教科書，論文を参照した．

[1] W. Buchholz and S. Wainer, Provably computable functions and the fast-growing hierarchy, *Contemporary Math. 65*, Amer. Math. Soc., 1987, pp. 179-198.

[2] M. Loebl and J. Nesetril, An unprovable Ramsey-type theorem, *Proc. Amer. Math. Soc.*, 1992, pp. 819-824.

[3] J. Paris and L. Harrington, A mathematical incompleteness in Peano arithmetic, *Handbook of Mathematical Logic*, North-Holland, 1972, pp. 1133-1142

[4] 竹内外史-八杉満利子著『証明論入門』共立出版 1988.

Part D.　算術の超準モデル

完全性定理によって対応付けられる形式的証明とモデルという二つの概念は，証明論とモデル論という数学基礎論の二つの分野を導く．不完全性定理の証明を見るまでもなく，算術の公理系の議論においては，古くから証明論が中心的な役割を果たしてきた．そもそもの算術の公理化の目的が算術の構文論的な分析にあり，しかもモデル論の展開には完全性定理の証明の後さらに相当の時間が必要だったことを考えると，これは当然のこととも言えよう．それが，数理哲学的な関心事であった公理系の無矛盾性などが数学基礎論の成熟と共に数学的な研究対象への変化していったように，数学基礎論での問題意識の持ち方や議論の方法は多様化し，算術についてもモデル論的な視点や手法による議論が積極的になされるようになった．

自然数の集合以外の算術のモデルを算術の超準モデルという．パート D では算術の超準モデルにまつわる幾つかの話題を見ていきたい．

第 14 講では算術の超準モデルの基本的な性質を紹介する．第 15 講では不完全性定理の成立と関係する算術の超準モデルの性質として，算術の超準モデルの演算は再帰的には定義は出来ないというテンネンバウムの定理を証明する．第 16 講では，算術の超準モデルを用いた第二不完全性定理の証明を紹介する．第 17 講では算術の超準モデルと計算量理論の関係についての一つの結果を紹介する．第 15 講から第 17 講までは互いに独立した内容を持つ．

算術の超準モデルに関する教科書に [1] や [2] がある．算術の超準モデルについて詳しくはこうした教科書を参照して欲しい．

第 14 講　算術の超準モデル

14.1　算術の超準モデル

自然数の集合 N を考える．

自然数上の和と積，二つの自然数 0, 1，自然数上の順序を自然数に関する基本的な構造と考える．これらの構造に対応する記号からなる一階述語論理の言語 $\mathcal{L}_A = (+, \cdot, 0, 1, <)$ を算術の言語と呼び，対応する自然数の集合 N による構造 $(\mathbf{N}, +, \cdot, 0, 1, <)$ を $\mathfrak{N}$ とする．$\mathcal{L}_A$ を用いた算術の公理化を考えたい．

注意．$\mathcal{L}_A$ の添え字 A は「算術 (arithmetic)」を意味する．第 2 講では同様の記号を違った意味で用いているが，$\mathcal{L}_A$ という記号を標準的なものと考え，あえてこの記号を用いることにする．また，以下では特に混乱のない限り，$\mathcal{L}_A$ の記号とその $\mathcal{L}_A$ の構造上での解釈を同じ文字で表す．たとえば，$\mathcal{L}_A$ の記号 $+$ に対応する $\mathfrak{N}$ 上の関数 $+^N$ を単に $+$ で表す．同様に構造 $\mathfrak{M}$ とその領域 $|\mathfrak{M}|$ を区別しない．

T を $\mathcal{L}_A$ の理論とする．算術の公理化として次の三つの性質が T に期待される．

1. T は $\mathfrak{N}$ をモデルに持つ．
2. $\mathfrak{N}$ 上で正しい $\mathcal{L}_A$ の文はすべて T から証明可能．
3. T は $\mathfrak{N}$ のみをモデルに持つ．

明らかに，T は条件 3 を満たせば条件 2 を満たし，条件 2 を満たせば条件 1 を満たす．条件 1 を満たさない理論は技術的な興味はあっても算術の公理化と呼べない．第一不完全性定理により，再帰的に公理化可能であって条件 2 を満たす T は存在しない．$\mathfrak{N}$ の上で正しい $\mathcal{L}_A$ の文全体から成る理論を **TA (True Arithmetic)** とすると TA は条件 2 を満たすので，再帰的に公理化可能という条件を外せば条件 2 を満たす T は自明に存在する．条件 3 を考える．

T を $\mathfrak{N}$ をモデルに持つ $\mathcal{L}_A$ の理論とする．レーベンハイム-スコーレムの定理によると，可算濃度のモデルを持つ形式的体系は任意の無限濃度のモデルを持ち，

$\mathfrak{N}$ は T の可算濃度のモデルなので T は連続濃度のモデル $\mathfrak{M}$ を持つ．$\mathfrak{M}$ と $\mathfrak{N}$ は明らかに同型でない．ゆえに T は $\mathfrak{N}$ 以外のモデルを持ち，条件 3 を満たす理論は存在しない．このことは一階の述語論理の言語を用いる限り $\mathcal{L}_A$ の定め方にはよらず，その意味で T が $\mathfrak{N}$ をモデルに持つとき必ず $\mathfrak{N}$ 以外のモデルを持つことは，一階の述語論理という言語体系の記述力のある意味での限界を示している．

$\mathfrak{N}$ と同型な T のモデルを**標準モデル (standard model)** といい，それ以外の T のモデルを T の**超準モデル (nonstandard model)** という．非可算の濃度の T のモデルはすべて超準モデルであるが，標準モデルは可算濃度の T のモデルとしても特徴付けられない．

定理 14.1　T が $\mathfrak{N}$ をモデルに持てば，T は可算濃度の超準モデルを持つ．

[証明]　c を新しい定数記号とし，算術の言語に c を付け加えた言語を $\mathcal{L}'_A$ とする．T に論理式の集合 $\{\bar{i} < c : i \in \mathfrak{N}\}$ ($\bar{i}$ は i の数項) を公理の集合として加えて得られる $\mathcal{L}'_A$ の理論を T' とする．T' が無矛盾であることを示したい．

S を T' の任意の有限部分集合とする．このとき自然数 n が存在して，

$$S \subseteqq T \cup \{\bar{i} < c : i \leqq n\}.$$

c を $n+1$ で解釈すると，$\mathfrak{N}$ は $T \cup \{\bar{i} < c : i \leqq n\}$ のモデル．よって S はモデルを持ち，コンパクト性定理から T' もモデルを持つ．

さて，レーベンハイム-スコーレムの定理から T' は可算濃度のモデル $\mathfrak{M}$ を持つ．$T \subseteqq T'$ より，明らかに $\mathfrak{M}$ は T のモデル．$\mathfrak{M}$ は $\mathcal{L}'_A$ 構造なので定数記号 c の $\mathfrak{M}$ 上での解釈 c^M があり，$\mathfrak{M} \models T'$ なので任意の自然数 i について $(\bar{i})^M < c^M$. よって $\mathfrak{M}$ と $\mathfrak{N}$ は同型でない．ゆえに $\mathfrak{M}$ は T の超準モデル．□

再帰的に公理化可能で無矛盾な算術の理論が超準モデルを持つことは第 16 講で見るように不完全性定理を用いて示すこともできる．

算術の超準モデルの存在が示されたのは不完全性定理の証明よりも古い．モデル論の発展に応ずるように 1960 年頃から算術の超準モデルが積極的に研究されるようになり，1970 年代に入ると算術の独立命題を探すことが算術の超準モデルを

用いてなされている．パリス (J. Paris) とハーリントン (L. Harrington) による命題もこの流れの中で発見されており，その独立性は算術の超準モデルを用いても証明できる．

14.2 ペアノ算術

自然数の集合を特徴付けるもっとも大切な性質は数学的帰納法である．$\phi(x)$ を $\mathcal{L}_A$ の論理式とするとき，次の形の論理式を ϕ に対する**帰納法の公理 (induction axiom)** と呼ぶ．

$$\phi(0) \land \forall x(\phi(x) \to \phi(x+1)) \to \forall x \phi(x)$$

以下の公理 (I), (II), (III) (順序を持つ半環の公理) からなる $\mathcal{L}_A$ の理論を $\mathbf{PA}^-$ と書く．

(I) 半環の公理．

(I-1) $\forall x\, \forall y\, \forall z\, ((x+y)+z = x+(y+z))$

(I-2) $\forall x\, \forall y\, (x+y = y+x)$

(I-3) $\forall x\, \forall y\, \forall z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z))$

(I-4) $\forall x\, \forall y\, (x \cdot y = y \cdot x)$

(I-5) $\forall x\, \forall y\, \forall z\, (x \cdot (y+z) = x \cdot y + x \cdot z)$

(I-6) $\forall x\, (x+0 = x \land x \cdot 0 = 0)$

(I-7) $\forall x\, (x \cdot 1 = x)$

(II) 0 を最小元とする離散的全順序の公理．

(II-1) $\forall x\, \neg(x < x)$

(II-2) $\forall x\, \forall y\, \forall z\, (x < y \land y < z \to x < z)$

(II-3) $\forall x\, \forall y\, (x < y \lor x = y \lor y < x)$

(II-4) $\forall x\, \neg\exists y\, (x < y < x+1)$

(II-5) $\forall x\, (0 = x \lor 0 < x)$

(III) 演算と順序の関係．

(III-1) $\forall x\, \forall y\, \forall z\, (x < y \to x+z < y+z)$

(III-2) $\forall x\, \forall y\, \forall z\, (0 < z \land x < y \to x \cdot z < y \cdot z)$

PA^- にすべての $\mathcal{L}_A$ の論理式に対する帰納法の公理を加えて得られる $\mathcal{L}_A$ の理論を **PA** (ペアノ算術，**Peano Arithmetic**) という．

注意．ここで与えた算術の言語，PA の定義は第 5 講で与えられたものとは異なるが，本質的な違いは無い．第 5 講の中ですでに一部述べられているように，ここでの算術の言語に現れる関数や関係はすべて第 5 講で定義された PA の中で定義可能であり，さらに，ここで与えた PA の公理はすべて第 5 講で与えた PA の公理から証明可能である．逆もまた成り立つ．また，PA の基礎になる理論として PA^- の代わりにロビンソンの Q が用いられることが多い．帰納法の公理があるときには PA^- は冗長なのがその理由の一つであるが，帰納法の公理がない理論を考えるときに Q では弱すぎる場合もあることから，最近では PA^- が用いられることも多い．

PA とは，いわゆるペアノの公理系の数学的帰納法の適用範囲を算術の言語で定義可能な集合に制限したものといえる．算術の言語で定義可能な概念を算術の初等的な命題と同一視すれば,「PA は完全か？」という問題は「正しい初等的な命題は全て初等的な命題に関する帰納法から証明可能か？」という問題と読むことができ，第一不完全性定理はこれに否定的に答える．

数学的帰納法の適用範囲にさらに制限を加えることで，PA の部分体系が得られる．論理記号 $\forall, \exists$ をまったく含まない論理式を**開 (open) 論理式**といい，$\exists$, $\forall$ が $\forall x < t$ や $\exists x < t$ の形のみで現れる $\mathcal{L}_A$ の論理式を Δ_0**論理式**という．上の PA の数学的帰納法の公理を $\phi(x)$ が開論理式，Δ_0論理式の場合に制限することで得られる PA の部分体系をそれぞれ **IOpen**, $\mathrm{I}\Delta_0$ という．第 17 章で見るように，$\mathrm{I}\Delta_0$ は計算量理論との関係を持つ．

さて，PA^- のモデルは順序 $<$ によって 0 を最小元とする全順序集合をなす．ある条件を満たす自然数が存在するとき，その条件を満たす最小の自然数が存在することはよく知られている $\mathbf{N}$ の性質である．この性質を**最小値原理 (least number principle)** という．PA 上では $\mathcal{L}_A$ の論理式で定義可能な集合に関する最小値原

理が成り立つ．

定理 14.2 (最小値原理) $\phi(x)$ を算術の論理式とする．このとき

$$\mathrm{PA} \vdash \exists x\ \phi(x) \to \exists x\ (\phi(x) \land \forall z < x \neg\phi(z)).$$

[証明] PA の中で議論する．対偶を証明する．$\neg\exists x\ (\phi(x) \land \forall z < x\ \neg\phi(z))$ とする．これを変形すると $\forall x(\neg\phi(x) \lor \neg\forall z < x\ \neg\phi(z))$ となり，$\forall x(\forall z < x\ \neg\phi(z) \to \neg\phi(x))$. したがって，$\forall x(\forall z < x\ \neg\phi(z) \to \forall z < x+1\ \neg\phi(z))$. また，0 は最小限なので，$\forall z < 0\ \neg\phi(z)$. よって，$x$ を自由変数に持つ論理式 $\forall z < x\ \neg\phi(z)$ に対する帰納法で $\forall x\ \forall z < x\ \neg\phi(z)$. ゆえに $\neg\exists x\ \phi(x)$. □

$\mathrm{I}\Delta_0$ 上では Δ_0論理式に対する最小値原理が証明可能である．$\mathrm{I}\Delta_0$ に全ての $\mathcal{L}_A$ の論理式に対する最小値原理を公理として加えた体系は PA と同等であり，この意味で $\mathrm{I}\Delta_0$ 上で最小値原理は数学的帰納法と等価である．一方，IOpen でも開論理式に対する最小値原理は成り立つが，このことの証明は定理 14.2 の証明程には明らかではない．

14.3 超準モデルの順序構造

以下，$\mathfrak{M}$ を PA の超準モデルとする．$\mathfrak{M}$ 上の二項関係 $<$ を考える．PA の公理から，$<$ は 0 を最小限とする離散的な全順序をなす．この節では PA の超準モデルの順序構造を詳しく見ていきたい．

まず，$\mathfrak{M}$ は各自然数 n の数項の解釈 $(\bar{n})^M$ を持つ．この $(\bar{n})^M$ と n を同一視して，$\mathfrak{N}$ を $\mathfrak{M}$ の部分集合と考える．順序 $<$ は離散的なので $\mathfrak{M} \models n < a < n+1$ を満たす $\mathfrak{M}$ の元 a は存在しない．よって $\mathfrak{M}$ は小さい方から自然数 $0, 1, 2, \cdots$ が並ぶ．(図 14.1)

$\mathfrak{M}$ は PA の超準モデルなので，$\mathfrak{M} \setminus \mathfrak{N}$ は空集合でない．a を $\mathfrak{M} \setminus \mathfrak{N}$ の元とする．a は任意の自然数 n に対して $\mathfrak{M} \models n < a$ を満たすので，$\mathfrak{M} \setminus \mathfrak{N}$ の元を $\mathfrak{M}$ の無限大 **(infinite)** 元，または超準 **(nonstandard)** 元と呼ぶ．a の後には $a+1, a+2, \ldots$ という $\mathfrak{M}$ の無限大元が続く．また，数学的帰納法により，PA 上

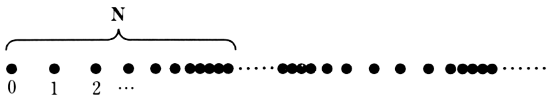


図 14.1

で $\forall x(0 < x \to \exists! y(y+1=x))$ が証明可能であり，a は $0 < a$ を満たすので $(a-1)+1=a$ を満たす $\mathfrak{M}$ の元 $a-1$ が存在する．もし $a-1$ が無限大元でないとすると a も無限大元でないので $a-1$ は無限大元．よって，$(a-2)+1=a-1$ を満たす $\mathfrak{M}$ の元 $a-2$ が存在する．同様に a の前には $\mathfrak{M}$ の無限大元 $a-1, a-2, \ldots$ が並ぶ．以上から，順序構造のみを考えたとき，a の前後には整数の集合 Z と同型な部分がある．(図 14.2)

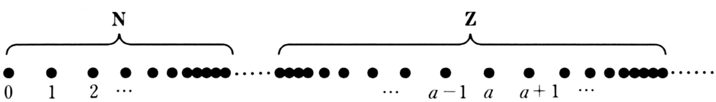


図 14.2

さて，$\mathfrak{M}' = \mathfrak{M} \setminus \mathfrak{N}$ とし，$\mathfrak{M}'$ の元 a, b について，ある自然数 n が存在して $|a-b| = n$ のとき $a \sim b$ と定める．$\sim$ は $\mathfrak{M}'$ 上の同値関係となるので，$\mathfrak{M}$ の無限大元全体は互いに重なり合わない Z と同型な部分集合の列から成ることが分かる．(図 14.3)

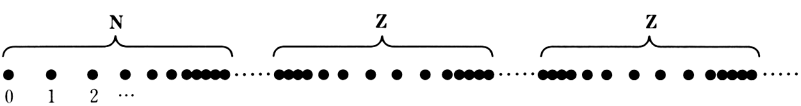


図 14.3

$\widetilde{\mathfrak{M}}$ を $\mathfrak{M}'/\sim$ とし，$a \in \mathfrak{M}'$ を含む $\widetilde{\mathfrak{M}}$ の同値類を $\tilde{a}$ で表わす．$\tilde{a}$ は $\mathfrak{M}'$ の中で a を含み Z と同型な部分をひとまとめにしたもので，それを並べたものが $\widetilde{\mathfrak{M}}$ である．任意の $\tilde{a}, \tilde{b} \in \widetilde{\mathfrak{M}}$ に対して

$$\tilde{a} < \tilde{b} \Leftrightarrow \mathfrak{M} \models a < b \text{ かつ } a \not\sim b$$

によって $\widetilde{\mathfrak{M}}$ 上の二項関係 $<$ を定義する．この定義が代表元の選び方によらないことは明らか．

定理 14.3 (1) $<$ は $\widetilde{\mathfrak{M}}$ 上の全順序．
(2) $\widetilde{a} < \widetilde{b}$ を満たす任意の $\widetilde{a}, \widetilde{b} \in \widetilde{\mathfrak{M}}$ に対し $\widetilde{c} \in \widetilde{\mathfrak{M}}$ が存在して $\widetilde{a} < \widetilde{c} < \widetilde{b}$.
(3) $\widetilde{\mathfrak{M}}$ は $<$ に関して端点を持たない．つまり最小限も最大限も持たない．
[証明] (1) は $\mathfrak{M}$ 上の順序 $<$ が全順序であることから明らか．

(2) $a, b \in \mathfrak{M}'$, $\widetilde{a} < \widetilde{b}$ とする．$\mathfrak{M} \models \exists x(a + b < 2x)$ より，最小値原理を用いて $\mathfrak{M} \models \exists x(a + b < 2x \wedge \forall y < x(2y \leqq a + b))$. よって $\mathfrak{M}$ の元 c が存在して $\mathfrak{M} \models a + b = 2c \vee a + b = 2c + 1$. このとき $\mathfrak{M} \models a < b$ より $\mathfrak{M} \models a < c < b$. もし $a \sim c$ または $b \sim c$ ならば $\widetilde{a} = \widetilde{b}$ となるので $\widetilde{a} < \widetilde{c} < \widetilde{b}$.

(3) $a \in \mathfrak{M} \setminus \mathfrak{N}$ とする．$\widetilde{a}$ が最小限でないことは (2) と同様に $\mathfrak{M} \models \exists x(a = 2x \vee a = 2x + 1)$ から明らか．a が最大限でないことは $\mathfrak{M} \models \widetilde{a} < \widetilde{2a}$ から明らか．

□

この定理の条件 (1), (2) を満たす順序を**稠密な全順序 (dense linear order)** という．以上から $\mathfrak{M}$ の順序型は A を端点を持たない稠密な全順序集合として

$$\mathfrak{M} \simeq \mathbf{N} + \mathbf{Z} \cdot A$$

となる．端点を持たない稠密な全順序集合は，可算の場合はすべて有理数の集合と同型である．(このことは明らかとは言えないかも知れないが，証明は難しくはない．[3] などを参照のこと．) よって PA の可算超準モデルの順序構造は完全に決定でき，それは $\mathfrak{N}$ 上の再帰的な関係として表現できる．

以上の議論は $\mathrm{I}\Delta_0$ の超準モデルについても同様に成り立つ．

14.4 始切片，終拡大

PA や $\mathrm{I}\Delta_0$ の超準モデルは全順序集合である．それを切断したものはさまざまで，$\mathcal{L}_A$ の構造にさえならない場合もあれば，$\mathrm{I}\Delta_0$ の超準モデルの切断が PA の超準モデルになることもある．超準モデルの切断が $\mathcal{L}_A$ の構造をなす場合，その切

断をもとのモデルの始切片と言う．ここでは，始切片の基本的な性質を紹介する．

定義．$\mathfrak{M}$ を $\mathcal{L}_A$ の構造とし，$\mathfrak{M}'$ をその部分構造とする．$\mathfrak{M} \setminus \mathfrak{M}'$ の任意の元 a と $\mathfrak{M}'$ の任意の元 b について $\mathfrak{M} \models b < a$ が成り立つとき $\mathfrak{M}'$ は $\mathfrak{M}$ の**始切片** **(initial segment)** である，または $\mathfrak{M}$ は $\mathfrak{M}'$ の**終拡大** **(end-extension)** であるといい，$\mathfrak{M}' \subseteq_e \mathfrak{M}$ と書く．

たとえば，PA の任意の超準モデル $\mathfrak{M}$ について $\mathfrak{N} \subseteq_e \mathfrak{M}$.

定理 14.4　$\mathfrak{M}' \subseteq_e \mathfrak{M}$ とする．このとき，任意の Δ_0論理式 $\phi(\overrightarrow{x})$ と $\mathfrak{M}'$ の任意の元 $\overrightarrow{a}$ について，$\mathfrak{M}' \models \phi(\overrightarrow{a})$ と $\mathfrak{M} \models \phi(\overrightarrow{a})$ は同値．

[証明]　論理式の複雑さに関する帰納法．□

ϕ を Δ_0論理式とする．$\exists x_1 \cdots \exists x_n\, \phi$ の形の論理式を Σ_1**論理式**，$\forall x_1 \cdots \forall x_n\, \phi$ の形の論理式を Π_1**論理式**という．

系 14.5　$\mathfrak{M}' \subseteq_e \mathfrak{M}$ とする．このとき，任意の Σ_1論理式 $\phi(\overrightarrow{x})$ と $\mathfrak{M}'$ の任意の元 $\overrightarrow{a}$ について，$\mathfrak{M}' \models \phi(\overrightarrow{a})$ ならば $\mathfrak{M} \models \phi(\overrightarrow{a})$.

系 14.6　T を Π_1文で公理化可能な算術の体系とし，$\mathfrak{M}$ を T のモデル，$\mathfrak{M}'$ を $\mathfrak{M}$ の始切片とする．このとき $\mathfrak{M}' \models T$.

第 17 章で見るように，$\mathrm{I}\Delta_0$ は Π_1文で公理化可能であり，系 14.6 はよく使われる $\mathrm{I}\Delta_0$ の超準モデルの構成方法の一つとなる．

系 14.5 から可導性条件の一つがただちに得られる．

定理 14.7　任意の Σ_1文 ϕ に対し，$\mathfrak{N} \models \phi$ ならば $\mathrm{PA} \vdash \phi$

[証明]　ϕ を $\mathfrak{N} \models \phi$ を満たす Σ_1文とする．$\mathfrak{M}$ を PA のモデルとする．$\mathfrak{N} \models \phi$ か

つ $\mathfrak{N} \subseteq_e \mathfrak{M}$ より $\mathfrak{M} \models \phi$. よって完全性定理から PA$\vdash \phi$. □

数学的帰納法の成立を算術の超準モデルの性質として表現したものが**過剰原理 (overspill principle)** である．このように，証明の手順である数学的帰納法を，ある条件を満たす無限大元の存在定理として表現できることに，超準モデルを用いることの特徴がある．

定理 14.8 (過剰原理) $\mathfrak{M}$ を PA の超準モデル，$\mathfrak{M}'$ をその始切片，$\phi(x, \overrightarrow{y})$ を $\mathcal{L}_A$ の論理式，$\overrightarrow{b}$ を $\mathfrak{M}$ の元とする．このとき，$\mathfrak{M}'$ の任意の元 a について $\mathfrak{M} \models \phi(a, \overrightarrow{b})$ ならば $\mathfrak{M} \backslash \mathfrak{M}'$ の元 c が存在して，$\mathfrak{M} \models \forall x < c\, \phi(x, \overrightarrow{b})$.

[証明] $\mathfrak{M} \models \neg\phi(a, \overrightarrow{b})$ を満たす $\mathfrak{M}$ の元 a が存在したとする．最小値原理により，そのような元で最小なもの c が存在する．このとき明らかに $c \notin \mathfrak{M}'$ で $\mathfrak{M} \models \forall x < c\, \phi(x, \overrightarrow{b})$. □

この定理はまた，PA の超準モデルの中で $\mathfrak{N}$ が算術の言語で定義可能でないことにも対応する．より一般に，次の系が成り立つ．

系 14.9 $\mathfrak{M}$ を PA の超準モデル，$\mathfrak{M}'$ をその始切片とする．このとき $\mathfrak{M}'$ は $\mathfrak{M}$ において $\mathcal{L}_A$ の論理式で定義可能でない．すなわち，任意の $\mathcal{L}_A$ の論理式 $\phi(x, \overrightarrow{y})$ と $\mathfrak{M}$ の元 $\overrightarrow{b}$ について $\mathfrak{M}' \neq \{a \in \mathfrak{M} : \mathfrak{M} \models \phi(a, \overrightarrow{b})\}$.

同様に $\mathrm{I}\Delta_0$ の超準モデルの上では Δ_0論理式に対する過剰原理が成り立ち，$\mathrm{I}\Delta_0$ の超準モデルの中で $\mathfrak{N}$ は Δ_0論理式では定義可能でない．(IOpen に関しても同様．)

第 15 講 テンネンバウムの定理

15.1　テンネンバウムの定理

PA の可算超準モデルの順序構造は再帰的な関係として表現できた．しかし，加法や乗法は再帰的な関係としては定めることができない，というのがテンネンバウム (S. Tennenbaum) の定理である．本講では，このテンネンバウムの定理を証明する．

まず，算術のモデルが再帰的であることを以下のように定める．

定義． $\mathfrak{M}$ を $\mathcal{L}_A$ の可算構造とする．再帰的な関数 $\oplus, \odot$ と自然数 n_0, n_1, 再帰的な関係 $\lhd$ が存在して $\mathfrak{M}$ が $(\mathbf{N}, \oplus, \odot, n_0, n_1, \lhd)$ と同型になるとき $\mathfrak{M}$ は**再帰的 (recursive)** であるという．

たとえば，(自明に) $\mathfrak{N}$ は再帰的な $\mathcal{L}_A$ の可算構造である．

定理 15.1 (テンネンバウム) PA は再帰的な超準モデルを持たない．

[証明] PA が再帰的なモデル $\mathfrak{M}$ を持つと仮定する．矛盾を導きたい．

証明の細部に入る前に，証明全体のあらすじを説明する．再帰的に枚挙可能だが再帰的に分離不能な集合を A, B とする．つまり，A, B は以下の条件を満たす再帰的に枚挙可能な自然数の集合である：

1. $A \cap B = \phi$,
2. $A \subseteqq C$ かつ $C \cap B = \phi$ を満たす再帰的な集合 C は存在しない．

A, B はともに再帰的に枚挙可能な集合なので，表現定理から以下を満たす Δ_0論理式 $\alpha(x, y)$, $\beta(x, y)$ が存在する：任意の自然数 n について

$$n \in A \ \Leftrightarrow\ \mathfrak{N} \models \exists y\, \alpha(n, y),$$

$$n \in B \ \Leftrightarrow\ \mathfrak{N} \models \exists y\, \beta(n, y).$$

さて，自然数 u に対して，自然数の集合 A_u, B_u をそれぞれ

$$n \in A_u \Leftrightarrow \mathfrak{N} \models n \leqq u \wedge \exists y < u\alpha(n, y),$$

$$n \in B_u \Leftrightarrow \mathfrak{N} \models n \leqq u \wedge \exists y < u\beta(n, y)$$

と定義する．明らかに $A_u \subseteqq A$ かつ $B_u \subseteqq B$ なので $A_u \cap B_u = \phi$. この $A_u \cap B_u = \phi$ という関係は u をパラメータとする Δ_0論理式で書け，任意の自然数 u について $\mathfrak{M} \models A_u \cap B_u = \phi$ が成り立つ．よって，過剰原理から $\mathfrak{M}$ の無限大元 a が存在して $\mathfrak{M} \models A_a \cap B_a = \phi$. ここで，$A_a$ や B_a は $\mathfrak{M}$ の中で考えているので $\mathfrak{N}$ の部分集合ではなく $\mathfrak{M}$ の部分集合となり，a は $\mathfrak{M}$ の無限大元なので $A \subseteqq A_a$, $B \subseteqq B_a$. 自然数の集合 C を

$$C = A_a \cap \mathbf{N}$$

と定義する．このとき $A \subseteqq C$ かつ $C \cap B = \phi$. C は $\mathfrak{M}$ の中で上に有界なので C は $\mathfrak{M}$ の中でコーディングでき，$\mathfrak{M}$ が再帰的という仮定から，このコーディングは $\mathfrak{M}$ の外で，つまり $\mathbf{N}$ 上で再帰的にデコーディングできる．このことから C は再帰的となり，A と B が再帰的に分離不能という条件に矛盾する．

では，証明の細部に入る．

(I) まず，上のあらすじに出てきた α, β を用いて Δ_0論理式 $\phi(u)$ を以下のように定義する：

$$\phi(u) \Leftrightarrow \forall x, y, z \leqq u \neg(\alpha(x, y) \wedge \beta(x, z)).$$

n を任意の自然数とする．$A \cap B = \phi$ より任意の自然数 $i, j, k \leqq n$ について $\mathfrak{N} \models \neg(\alpha(i, j) \wedge \beta(i, k))$, つまり $\mathfrak{N} \models \phi(n)$. ϕ は Δ_0論理式かつ $\mathfrak{N} \subseteqq_e \mathfrak{M}$ なので $\mathfrak{M} \models \phi(n)$. $\mathfrak{M} \models \mathrm{PA}$ より $\mathfrak{M}$ は過剰原理を満たすので，$\mathfrak{M}$ の無限大元 a が存在して $\mathfrak{M} \models \phi(a)$.

自然数の集合 C を

$$C = \{n \in \mathfrak{N} : \mathfrak{M} \models \exists y \leqq a\alpha(n, y)\}$$

によって定める．$A \subseteqq C$ かつ $B \cap C = \phi$ を示したい．

$n \in A$ とする．このとき $\mathfrak{N} \models \exists y\, \alpha(n, y)$ なので，自然数 m が存在して $\mathfrak{N} \models \alpha(n, m)$. α は Δ_0論理式で $\mathfrak{N} \subseteqq_e \mathfrak{M}$ なので $\mathfrak{M} \models \alpha(n, m)$. $\mathfrak{M} \models m < a$ より $\mathfrak{M} \models \exists y \leqq a\, \alpha(n, y)$. よって $n \in C$. 以上から $A \subseteqq C$. 次

に $n \in B$ とする．このとき $\mathfrak{N} \models \exists y\, \beta(n,y)$ なので，$\mathfrak{M} \models \exists z \leqq a\, \beta(n,z)$. $\mathfrak{M} \models \phi(a)$ かつ $\mathfrak{M} \models n < a$ から $\mathfrak{M} \models \neg\exists y \leqq a\alpha(n,y)$. よって $n \notin C$. 以上から $B \cap C = \phi$.

(II), (III) で $\mathfrak{M}$ が再帰的であることを用いて C が再帰的となることを示す．C が再帰的なことは A, B が再帰的に分離不能であることに矛盾するので，テンネンバウムの定理が証明されたことになる．

(II) C を $\mathfrak{M}$ の無限大元を用いてコーディングする．

n 番目の素数を $\mathrm{p}(n)$ と書く．つまり，$\mathrm{p}(0) = 2, \mathrm{p}(1) = 3, \mathrm{p}(2) = 5, \ldots$. 二項関係 $\mathrm{p}(n) = m$ は再帰的なので，Δ_0論理式 $\theta(u,v,w)$ が存在して

$$\mathrm{p}(n) = m \;\Leftrightarrow\; \mathfrak{N} \models \exists w\, \theta(n,m,w).$$

この θ を用いて Δ_0論理式 $\psi(r)$ を

$$\psi(r) \;\Leftrightarrow\; \exists s \leqq a\, \forall u \leqq r\, \exists v, w \leqq a[\theta(u,v,w) \wedge (v|s \leftrightarrow u \in C)]$$

によって定義する．ただし $v|s, u \in C$ はそれぞれ $\exists t \leqq s(v \cdot t = s), \exists y \leqq a\, \alpha(u,y)$ の略記で，明らかに n が C の元であることと $\mathfrak{M} \models n \in C$ は同値．このとき n を任意の自然数とすると $\mathfrak{N} \models \psi(n)$ が成り立つので $\mathfrak{M} \models \psi(n)$. よって，過剰原理から $\mathfrak{M}$ の無限大元 b が存在し，$\mathfrak{M} \models \psi(b)$. すなわち $\mathfrak{M}$ の元 s が存在して

$$\mathfrak{M} \models \forall u \leqq b\, \exists v, w \leqq a[\theta(u,v,w) \wedge (v|s \leftrightarrow u \in C)].$$

ゆえに，任意の自然数 n について $\mathfrak{M} \models \mathrm{p}(n)|s$ と $n \in C$ が同値となり，s によって C はコーディングされたことになる．

同様に，$\exists y \leqq a\, \alpha(u,y)$ の代わりに $\neg\exists y \leqq a\, \alpha(u,y)$ を考えることによって $\mathfrak{M}$ の元 s' の存在して，任意の自然数 n について $\mathfrak{M} \models \mathrm{p}(n)|s'$ と $n \in \mathbf{N} \setminus C$ が同値となることが示される．

(III) さて，今度は s, s' のデコーディングをする．$\mathfrak{M}$ が再帰的であるという仮定から，このデコーディングによって C が再帰的であることが示される．

$\mathfrak{M}$ は PA の再帰的な可算モデルなので，再帰的な関数 $\oplus, \odot$ と自然数 n_0, n_1, 再帰的な関係 $\lhd$ が存在して $\mathfrak{M}$ は $(\mathbf{N}, \oplus, \odot, n_0, n_1, \lhd)$ と同型．$f : \mathfrak{M} \to \mathbf{N}$ をその同型を与える写像とする．s のデコーディングにこの

$(\mathbf{N}, \oplus, \odot, n_0, n_1, \lhd)$ を用いる．

ところで，自然数 n は通常の n 番目の自然数と，$\mathfrak{M}$ の元に対応する元という二通りの意味を持ち，$m \odot n$ は n 個の m を $\oplus$ で結ぶものを意味せず，$f(k) = n$ を満たす $k \in \mathfrak{M}$ について k 個の m を $\oplus$ で結ぶものを意味する．よって，デコーディングに $\odot$ を直接用いることはできない．そこで，新たに関数 $\otimes : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ を

(a) $m \otimes 0 = n_0$

(b) $m \otimes (n+1) = (m \otimes n) \oplus m$

によって定義する．$\oplus$ が再帰的なので $\otimes$ は再帰的となる．(ここで $\mathfrak{M}$ が再帰的であるという仮定を使う．) この $\otimes$ は $\mathfrak{M}$ の元 k, l と自然数 n について

$$\mathfrak{M} \models k \cdot n = l \;\Leftrightarrow\; \mathfrak{N} \models f(k) \otimes n = f(l)$$

を満たす．この $\otimes$ を用いて，自然数の集合 $\widetilde{C}$ を

$$\widetilde{C} = \{n \in \mathfrak{N} : \mathfrak{N} \models \exists t(t \otimes n = f(s))\}$$

と定める．明らかに $\widetilde{C}$ は再帰的に枚挙可能．このとき $\mathfrak{M}$ の任意の元 t と自然数 n について

$$\mathfrak{M} \models t \cdot n = s \;\Leftrightarrow\; \mathfrak{N} \models f(t) \otimes n = f(s)$$

が成り立つので，任意の自然数 n について

$$\mathfrak{M} \models n | s \;\Leftrightarrow\; n \in \widetilde{C}.$$

したがって

$$n \in C \;\Leftrightarrow\; \mathrm{p}(n) \in \widetilde{C}.$$

ゆえに C は再帰的に枚挙可能な集合．

s の代わりに s' を考えることで，同様に $\mathbf{N} \setminus C$ も再帰的に枚挙可能な集合であることが示される．ゆえに C は再帰的集合となり，矛盾．以上でテンネンバウムの定理が証明された．□

$\mathfrak{M}$ の無限大元 a によって与えられる集合 C と $\mathbf{N} \setminus C$ が $\mathfrak{M}$ の無限大元によってコーディングできることが，この証明のポイントになっている．自然数によってコーディングされる自然数の集合は有限集合なので，当然再帰的となる．$\mathfrak{M}$ が再

帰的であれば，$\mathfrak{M}$ の無限大元でコーディングされる自然数の集合も再帰的となる．

15.2　再帰的な超準モデルについて

前節の証明は $\oplus$ が再帰的なことしか用いていないので，それは PA が加法のみを再帰的とする超準モデルも持たないことの証明になっている．コーディングの方法を変えることで，同様に PA は乗法のみが再帰的な超準モデルも持たないことが示される．PA の超準モデルの加法や乗法は順序構造と比べはるかに複雑である．

$\mathrm{I}\Delta_0$ は PA よりも弱いので PA よりも多くのモデルを持つが，$\mathrm{I}\Delta_0$ も再帰的な超準モデルを持たないことをマカルーン (K. McAloon) が証明している．前節で紹介したテンネンバウムの定理の証明では，二ケ所で PA のモデル $\mathfrak{M}$ が帰納法を満たすことを用いている．一つは (I) で $\mathfrak{M} \models \phi(a)$ を満たす無限大元 a の存在を示すところで，もう一つは (II) で $\mathfrak{M} \models \psi(b)$ を満たす無限大元 b の存在を示すところである．いずれも Δ_0論理式に対する過剰原理を用いており，それは $\mathfrak{M}$ が $\mathrm{I}\Delta_0$ を満たすときに成り立つ．よって，前節の証明はそのまま $\mathrm{I}\Delta_0$ が再帰的な超準モデルを持たないことの証明となる．

これに対し，IOpen は再帰的な超準モデルを持ち，その意味で IOpen は PA や $\mathrm{I}\Delta_0$ と比べ本当に弱い．シェファードソン (J.C. Shepherdson) は IOpen のモデルの代数的な特徴付けをして IOpen の再帰的な超準モデルを構成し，IOpen からは素数が無限に存在することなどが証明できないことを示した．後に，さらに有効な IOpen のモデルの構成方法がウィルキー (A. Wilkie) によって示され，それをもとにマッキンタイア (A. Macintyre) とマーカー (D. Marker) は素数が無限に存在することだけでなく，IOpen では素数に関する性質はほとんど何も証明できないことを示している．

前節のテンネンバウムの定理の証明では再帰的に枚挙可能だが再帰的に分離不能な集合が用いられている．こうした集合の存在は本質的に第一不完全性定理と同値である．逆にテンネンバウムの定理から第一不完全性定理を導くことも可能であり，テンネンバウムの定理は第一不完全性定理をモデルの言葉で表わした定

理といえる．(詳しくは [1] を参照のこと．) 完全性定理によると，ある命題が PA から証明可能でないことを示すためには，その命題を成り立たせないモデルの存在を示せばいい．しかし一般に，ある条件を満たすモデルを構成することはとても難しい．再帰的な PA のモデルが存在しないことが，その難しさの原因の一つである．

PA や $I\Delta_0$ は再帰的な超準モデルを持たないので，PA や $I\Delta_0$ の超準モデルを作るときには完全性定理などによってあらかじめ素材となるべきモデルを用意し，必要に応じてそのモデルを伸ばしたり (end-extension を構成したり) 切ったり (initial segment を作ったり) することになる．第 16 講では「伸ばして」第二不完全性定理を証明する．第 17 講では「切って」パリクの定理と呼ばれる定理を証明する．

第16講 モデルを用いた不完全性定理の証明

16.1 不完全性定理と超準モデル

第14講ではコンパクト性定理を用いて算術の超準モデルの存在を示した．PAが超準モデルを持つことは以下のように第二不完全性定理を用いても証明できる．

[第二不完全性定理を用いた証明]　まず，$\mathfrak{N}$ は PA のモデルなので，完全性定理から PA は無矛盾．よって，PA が無矛盾であることを意味する論理式 Con(PA) は正しい．すなわち $\mathfrak{N} \models \mathrm{Con(PA)}$. また，第二不完全性定理から Con(PA) は PA から証明できない．よって $\mathrm{PA} + \neg\mathrm{Con(PA)}$ は無矛盾なのでモデル $\mathfrak{M}$ をもつ．$\mathfrak{M} \models \neg\mathrm{Con(PA)}$ なので $\mathfrak{M} \not\equiv \mathfrak{N}$. ゆえに $\mathfrak{M}$ は PA の超準モデル．□

この証明は第14講での証明といくつかの点で大きく異なる．第14講での証明では得られたモデルが $\mathfrak{N}$ と同型でないことが超準元の存在から直接示されるのに対し，上の証明では $\mathfrak{M}$ が $\mathfrak{N}$ と初等的には同値でないことを用いられており，その意味では間接的である．このことにより，第14講の証明の場合とは異なり，不完全性定理を用いる方法では完全な理論である TA が超準モデルを持つことを示すことはできない．

さて，上の証明とは逆に，Con(PA) を成り立たせない PA の超準モデルの存在を示すことができれば完全性定理から第二不完全性定理が得られる．しかし，テンネンバウムの定理により何も無いところから PA のモデルを直接構成するのは難しい．そこで Con(PA) を成り立たない PA の超準モデルを作るためにはまず Con(PA) を成り立たせる PA の超準モデルを用意することになる．しかし，Con(PA) は Π_1 文なので，Con(PA) を成り立たせる超準モデルの始切片では再び Con(PA) が成り立ち，算術の超準モデルの始切片は第二不完全性定理の証明には役に立たない．この講では算術化された完全性定理を用いて算術の超準モデルの終拡大を作り，第二不完全性定理を証明する．

16.2 完全性定理の算術化

完全性定理は通常，定理自身もその証明も集合論の言葉を用いて表される．その証明には選択公理が用いられているし，そもそもモデルという概念自体が集合概念によって表現される．しかし実際には，他の多くの数学の定理と同様，完全性定理に集合論の「言葉」が不可欠なわけではない．完全性定理が対象とする言語や理論は多くの場合ゲーデル数を用いて自然数上にコーディングが可能であり，完全性定理の証明も PA 上で展開できる．つまり，集合論の代わりに算術の中で完全性定理とその証明を表すことが可能である．この節ではそのことを見ていきたい．

完全性定理は「無矛盾ならモデルを持つ」という定理である．完全性定理を PA の上で展開するためには，モデルという概念を算術の言語で表現し，完全性定理自身を算術の言語で表現しなければならない．しかし，モデルとは構造を持つ集合なので，このことは直接には実行できない．そこで，モデルを考える代わりにモデルの上で成り立つ論理式全体から成る集合（モデル論でいう elementary diagram）を考え，その集合が PA 上で定義可能であることを PA 上に算術化された完全性定理とみなす．

では，より具体的に算術化された完全性定理を見ていきたい．まず $\mathcal{L}$ を一階の述語論理の言語とし，$\mathcal{L}$ 上にゲーデル数 $\ulcorner\ \urcorner$ が定められ，x が $\mathcal{L}$ の項，論理式，文のゲーデル数であるという意味の論理式 $trm(x)$, $fml(x)$, $snt(x)$ が Σ_1 論理式で書けるとする．次に T を再帰的に公理化可能な $\mathcal{L}$ 上の理論とし，$T(x)$ を「X は T の公理のゲーデル数である」という意味の Σ_1論理式とする．これらの論理式を用いると,「x は T で証明可能な論理式のゲーデル数である」「T は無矛盾である」という意味の Σ_1論理式 $\mathrm{Pr}_T(x)$, Π_1論理式 $\mathrm{Con}(T)$ が書ける．

次に，モデルの上で成り立つ論理式全体を論理式で表す．T' が T の拡大で，任意の論理式 $\phi(x)$ に対して $\phi(x)$ に現れていない定数 c が存在して

$$T' \vdash \exists x\, \phi(x) \to \phi(c)$$

が成り立つとき，T' を T の**ヘンキン拡大**という．完全性定理の証明では，T が

無矛盾のとき T がモデルを持つことを次の手順で示した．

1. T のヘンキン拡大 T' をつくる．
2. T' を含む完全な理論 T'' をつくる．
3. T'' をもとに，定数記号を用いてモデルをるくる．

この三番目の手順を省略し，二番目までを実行すること，つまり，T'' を定義する $\mathcal{L}_A$ の論理式 $T''(x)$ を作り，それが望ましい性質を持つことを PA 上で証明することが算術化された完全性定理の証明となる．

注意． 第 3 講での完全性定理の証明は一番目の手順と二番目の手順を交互に無限回繰り返している．しかし，ヘンキン拡大の作り方を工夫をすることで，それぞれの手順を一度ずつで済ますことができる．

T のヘンキン拡大 T' をつくるために，新しい定数記号の可算無限集合 $\mathcal{C}$ を用意し，$\mathcal{L}' = \mathcal{L} \cup \mathcal{C}$ によって言語を拡張する．このとき，もとの $\mathcal{L}$ のゲーデル数を適当に選び，$\mathcal{L}$ のゲーデル数の拡張となるように $\mathcal{L}'$ のゲーデル数を定める．x が $\mathcal{L}'$ の項，論理式，文のゲーデル数であるという意味の Σ_1論理式を $trm'(x), fml'(x), snt'(x)$ とする．$\mathcal{L}'$ のゲーデル数を適当に選ぶと T は再帰的に公理化可能なヘンキン拡大 T' を持ち,「X は T' の公理のゲーデル数である」,「x は T' で証明可能な論理式のゲーデル数である」という意味の Σ_1論理式 $T'(x)$, $\mathrm{Pr}_{T'}(x)$ が存在する．T' が T の保存的拡大になることは通常の証明とまったく同様に PA 上で証明できる．つまり，$\mathrm{PA} \vdash \forall x(snt(x) \land \mathrm{Pr}_{T'}(x) \to \mathrm{Pr}_T(x))$. また，$\mathrm{Con}(T')$ を「T は無矛盾である」という意味の Π_1文とすると，このことから $\mathrm{PA} \vdash \mathrm{Con}(T) \to \mathrm{Con}(T')$ がいえる．

さて，次に $T'(x)$ をもとに $T''(x)$ を作りたい．通常の証明では T'' の存在の証明に選択公理を用いるが，T'' が $\mathcal{L}_A$ の論理式で定義可能なことを示すために，選択公理の代わりに無限二分木が無限の長さの枝を持つこと（弱いケーニッヒの補題）を使う．まず，$\mathcal{L}'$ の文全体を並べて $\phi_0, \phi_1, \phi_2, \ldots$ とし，次の形の無限二分木を作る．(図 16.1)

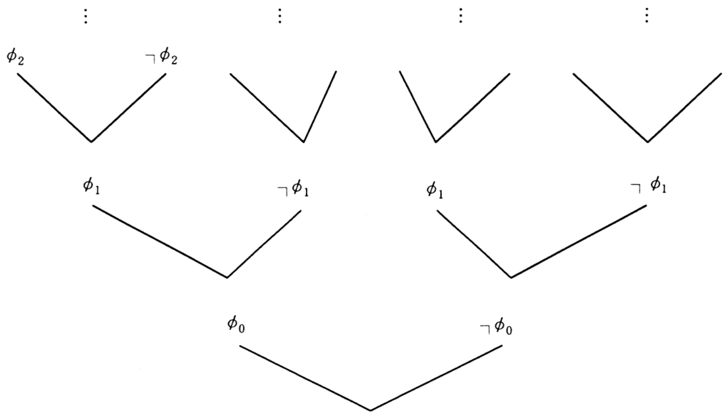


図 16.1

次に，この二分木の枝（たとえば $\phi_0 - \neg\phi_1 - \phi_2\}$）と，その枝の上に乗る文から成る集合（$\{\phi_0, \neg\phi_1, \phi_2\}$）を同一視し，$T'$ と無矛盾な理論を定める枝を集めて部分二分木を作る．T' が無矛盾という仮定から，この部分二分木は無限二分木となる．弱いケーニッヒの補題により，この二分木は無限の長さの枝を持ち，この枝の定める理論が T'' となる．このとき，無限の長さの枝は複数存在し得るが，その中でもっとも「左側」にあるものを選ぶことにする．この枝は $\mathcal{L}_A$ の論理式で定義可能なので，T'' を定める $\mathcal{L}_A$ の論理式 $T''(x)$ の存在がいえる．

このように定めた論理式 $T''(x)$ を以後 $Tr_T(x)$ と書く．この $Tr_T(x)$ があるモデルの上で正しい論理式全体を定めることを示すためには次のことを示せばいい．

$$\forall x(Pr_T(x) \to Tr_T(x))$$

$$\forall x(fml'(x) \to (Tr(\neg x) \leftrightarrow \neg Tr_T(x)))$$

$$\forall x, y(fml'(x) \land fml'(y) \to (Tr_T(x \land y) \leftrightarrow Tr_T(x) \land Tr_T(y)))$$

$$\forall x, y(fml'(x) \land fml'(y) \to (Tr_T(x \lor y) \leftrightarrow Tr_T(x) \lor Tr_T(y)))$$

$$\forall x, y(fml'(x) \to (Tr_T(\exists y(x)) \leftrightarrow \exists z(C(z) \to Tr_T(x[z/y]))))$$

$$\forall x, y(fml'(x) \to (Tr_T(\forall y(x)) \leftrightarrow \forall z(C(z) \to Tr_T(x[z/y])))).$$

ただし $x \land y$ などは「ゲーデル数 x の論理式とゲーデル数 y の論理式を $\land$ で

結んでできる論理式のゲーデル数」などのことであり，また $C(x)$ は「x は $\mathcal{C}$ の元のゲーデル数である」を意味する論理式である．これらの論理式を「かつ」で結ぶことでできる論理式を $\mathrm{Mod}_T(Tr_T)$ と書く．そして，$\mathrm{Con}(T)$ を仮定すれば $\mathrm{Mod}_T(Tr_T)$ が成り立つことは通常の完全性定理の証明の方法と同様に PA 上で証明できる．これが算術化された完全性定理である．

定理 16.1 (算術化された完全性定理) $\mathrm{PA} \vdash \mathrm{Con}(T) \rightarrow \mathrm{Mod}_T(Tr)$.

16.3　モデルを用いた不完全性定理の証明

算術化された完全性定理を用いて不完全性定理を証明することの歴史は古く，クライゼル（G. Kreisel）は 1950 年代に算術化された完全性定理を用いて第一，第二不完全性定理を導いている．算術化された完全性定理を用いることで不完全性定理の証明でモデルを用いる議論が可能となる．モデルを用いることでいわゆる「有限の立場」と呼ばれる枠組みから外に出てしまうが，集合概念や代数的な構造に慣れていれば，すべてをシンタックスだけで話しを進めるより証明の見通しが良くなる場合もある．不完全性定理，特に第二不完全性定理の証明には「証明の形式化，証明の形式化の形式化」などが出てくる．一つ一つの形式化に対してモデルの構成を行うことで，その形式化されたものは形式の外に出て，何層にもわたる形式化を同時に考える必要はなくなる．

以下でイェック（T. Jech）による第二不完全性定理のモデル論的な証明を紹介する．原典は [4]. ただし，イェック自身の証明は集合論に対する第二不完全性定理のものであり，PA などの算術の体系のものではない．よって，その証明で使われるのは「算術化」されていない，通常の完全性定理である．本講で紹介する証明はイェックの証明を PA に対するものに書き直したものであり，そのとき，集合論の言葉で書かれた通常の完全性定理に対応するものとして「算術化された完全性定理」が用いられる．

なお，この節では PA が無矛盾であることを自明な事実として仮定する．また，

ここで与える証明は PA を含み無矛盾で再帰的に公理化可能な $\mathcal{L}_A$ の理論であれば，PA 以外のものにもそのまま適用できる．

定義. $\mathfrak{M}$ を PA のモデルとし，$\mathfrak{M}'$ を $\mathfrak{M} \subseteq_e \mathfrak{M}'$ を満たす $\mathcal{L}_A$ の理論 T のモデルとする．論理式 $Tr(x)$ が存在して次の二条件が成立するとき $\mathfrak{M}'$ は $\mathfrak{M}$ 上で定義可能な T のモデルであるといい，$\mathfrak{M} \subseteq_T \mathfrak{M}'$ と書く．

1. 任意の $\mathcal{L}_A$ の文 ϕ について，$\mathfrak{M} \models Tr(\ulcorner\phi\urcorner)$ と $\mathfrak{M}' \models \phi$ が同値．
2. 任意の $\mathcal{L}_A$ の文 ϕ について，$\mathfrak{M} \models \mathrm{Pr}_T(\ulcorner\phi\urcorner)$ ならば $\mathfrak{M}' \models \phi$

条件 1 は $\mathfrak{M}'$ 上の真偽が $\mathfrak{M}$ 上で定めらることを意味する．条件 2 は $\mathfrak{M}$ 上で T から証明可能な論理式はすべて $\mathfrak{M}'$ 上で正しい，すなわち $\mathfrak{M}$ 上で $\mathfrak{M}'$ が T のモデルになることを意味する．

算術化された完全性定理から次の定理が得られる．

定理 16.2 T を PA を含む算術の理論とする．ことのき $\mathrm{PA} + \mathrm{Con}(T)$ の任意のモデル $\mathfrak{M}$ に対して $\mathfrak{M} \subseteq_T \mathfrak{M}'$ を満たす T のモデル $\mathfrak{M}'$ が存在する．

この定理は $\mathfrak{M} \subseteq_T \mathfrak{M}'$ の定義に現れる論理式 $Tr(x)$ として算術化された完全性定理の証明で与えられる $Tr_T(x)$ を用い，$\mathfrak{M}$ の構造と $Tr_T(x)$ により集合 $\mathfrak{M}$ の上に新しい構造 $\mathfrak{M}'$ を定義することで証明される．

定理 16.3 Con(PA) を成り立たせない PA のモデルが存在する．

[証明] PA の任意のモデルの上で Con(PA) が成り立つとする．矛盾を導きたい．まず，対角化定理より

$$\mathrm{PA} \vdash \sigma \leftrightarrow \neg \mathrm{Pr}_{\mathrm{PA}}(\ulcorner\sigma\urcorner)$$

を満たす算術の文 σ が存在．$\mathfrak{M}$ を PA のモデルとするとき，$\mathfrak{M} \models \sigma$ のとき $\mathfrak{M}$ は正であると，そうでないとき $\mathfrak{M}$ は負であると定める．

PA は無矛盾なので PA のモデル $\mathfrak{M}_1$ が存在する．もし $\mathfrak{M}_1$ が正ならば $\mathfrak{M}_1 \models$

$\neg \mathrm{Pr_{PA}}(\ulcorner\sigma\urcorner)$ なので $\mathfrak{M}_1 \models \mathrm{Con}(\mathrm{PA}+\neg\sigma)$. よって定理 16.2 から $\mathfrak{M}_1 \subseteq_{\mathrm{PA}+\neg\sigma} \mathfrak{M}_2$ を満たす $\mathrm{PA}+\neg\sigma$ のモデル $\mathfrak{M}_2$ が存在する．このとき，明らかに $\mathfrak{M}_2$ は負．もしも $\mathfrak{M}_1$ が負のときは $\mathfrak{M}_2 = \mathfrak{M}_1$ とする．ゆえに，負のモデル $\mathfrak{M}_2$ の存在が示された．

仮定より PA 任意のモデルの上で Con(PA) が成り立つので $\mathfrak{M}_2 \models \mathrm{Con}(\mathrm{PA})$. よって，再び定理 16.2 から $\mathfrak{M}_2 \subseteq_{\mathrm{PA}} \mathfrak{M}_3$ を満たす PA のモデル $\mathfrak{M}_3$ の存在がいえる．$\mathfrak{M}_2$ は負なので $\mathfrak{M}_2 \models \mathrm{Pr_{PA}}(\ulcorner\sigma\urcorner)$. よって $\mathfrak{M}_3 \models \sigma$. 一方，$\mathfrak{M}_2 \models \neg\sigma$ かつ $\mathfrak{M}_2 \subseteq_e \mathfrak{M}_3$ であり，$\neg\sigma$ は Σ_1文なので $\mathfrak{M}_3 \models \neg\sigma$. 矛盾．□

系 16.4　$\mathrm{PA} \nvdash \mathrm{Con}(\mathrm{PA})$.

[証明]　前の定理と完全性定理から明らか．□

じつは，定理 16.2 により，定理 14.7 を PA 上に形式化したもの

$$\mathrm{PA} \vdash \sigma \to \mathrm{Pr_{PA}}(\ulcorner\sigma\urcorner)$$

(ただし σ は Σ_1文）が証明できる．このことから可導性条件を用いる古典的な第二不完全性定理の証明をモデル論的なものに書き直すことができ，上の証明をそうしたものの一つとみなすこともできる．その意味では，上の証明は新しくはない．しかし，何重にも入れ子になった証明の形式化が必要となる不完全性定理の新しい証明を考えるときには，モデルを使うことの効果は小さくない．

算術化された完全性定理については [5] を参照のこと．

第 17 講 超準モデルと計算量理論

17.1 パリクの定理

再帰的関数とは原理的に計算可能な関数である．ここで「原理的に」とは，計算に必要な時間もメモリの量も無制限に使って構わないという条件が仮定される．原理的に計算可能であっても，計算結果を出すのに時間がかかり過ぎるなど，現実には計算可能とは言えない関数もある．第 14 講で定義した **PA** の部分体系 $\mathrm{I}\Delta_0$ は，この「現実に計算可能」という概念についての考察の中から 1971 年にパリクによって導入された体系である．1980 年代に入ってからパリス，ウィルキー，バス (S. Buss), 竹内外史らによって $\mathrm{I}\Delta_0$ 周辺の体系と計算量理論と関係が積極的に研究されており，それは**限定算術 (bounded arithmetic)** と呼ばれる数学基礎論の一分野を成している．

さて，再帰的関数 (のグラフ) は $\mathcal{L}_A$ の論理式で書き表すことが可能である．定義域が自然数全体であることを $\mathrm{I}\Delta_0$ で証明できる再帰的関数の値は，その関数の入力に対して多項式で押さえることが出来るというのがパリク (R. Parikh) の定理である．パリクの定理から，$\mathrm{I}\Delta_0$ では指数関数など多項式よりも早く増加する関数は扱えないことが分かる．本節ではこのパリクの定理を証明する．

補題 17.1 $\mathrm{I}\Delta_0$ は Π_1論理式で公理化可能．

[証明] $\phi(x)$ を Δ_0論理式とする．このとき ϕ に対する帰納法は次の論理式と同値：

$$\forall x(\phi(0) \land \forall y < x(\phi(y) \to \phi(y+1)) \to \phi(x)).$$

よって $\mathrm{I}\Delta_0$ は Π_1論理式で公理化可能．□

定理 17.2 (パリク) $\phi(x,y)$ を Δ_0論理式とする．このとき，もし

$$\mathrm{I}\Delta_0 \vdash \forall x\, \exists y\, \phi(x,y)$$

なら $\mathcal{L}_A$ の項 $t(x)$ が存在して

$$\mathrm{I}\Delta_0 \vdash \forall x\, \exists y < t(x)\, \phi(x,y).$$

[証明] 対偶を証明する．任意の項 $t(x)$ について

$$\mathrm{I}\Delta_0 \nvdash \forall x\, \exists y < t(x)\, \phi(x,y)$$

と仮定する．$\mathrm{I}\Delta_0 \nvdash \forall x\, \exists y\, \phi(x,y)$ を示したい．

まず，c を新しい定数記号とし，$\mathcal{L}_A$ の理論 T を

$$T = \mathrm{I}\Delta_0 \cup \{\forall y < t(c)\, \neg\phi(c,y) : t(x) \text{ は } \mathcal{L}_A \text{ の項}\}$$

によって定義する．T が無矛盾であることを示したい．T が矛盾すると仮定する．コンパクト性定理から算術の言語の項 $t_1, \ldots, t_n$ が存在して，

$$\mathrm{I}\Delta_0 \cup \{\forall y < t_i(c)\, \neg\phi(c,y) : i = 1, \ldots, n\}$$

は矛盾する．よって $\mathrm{I}\Delta_0 \vdash \bigvee_{i=1}^{n} \exists y < t_i(c)\, \phi(c,y)$. $t(x) = t_1(x) + \cdots + t_n(x)$ とおくと $\mathrm{I}\Delta_0 \vdash \exists y < t(c)\, \phi(c,y)$. c は新しい定数記号だったので $\mathrm{I}\Delta_0 \vdash \forall x\, \exists y < t(x)\, \phi(x,y)$ となり仮定に矛盾．

T は無矛盾なのでモデル $\mathfrak{M}$ をもつ．$a = \max\{2, c\}$ と定め，$\mathfrak{M}' \subseteq \mathfrak{M}$ を

$$\mathfrak{M}' = \{b \in \mathfrak{M} : \mathfrak{M} \models b < a^n, n \in \mathfrak{N}\}$$

によって定義する．$\mathfrak{M}'$ は和，積について閉じているので $\mathcal{L}_A$ の構造となり，また定義から明らかに $\mathfrak{M}' \subseteq_e \mathfrak{M}$. 補題 17.1 から $\mathrm{I}\Delta_0$ は Π_1論理式で公理化可能なので，定理 14.6 から $\mathfrak{M}' \models \mathrm{I}\Delta_0$. $\mathfrak{M}' \models \neg\exists y\, \phi(c,y)$ を示したい．

$\mathfrak{M}'$ の元 d が存在して $\mathfrak{M}' \models \phi(c,d)$ と仮定する．ϕ は Δ_0論理式なので $\mathfrak{M} \models \phi(c,d)$. $\mathfrak{M}'$ の定め方から $\mathcal{L}_A$ の項 $t(x)$ が存在して $\mathfrak{M} \models d < t(c)$. ゆえに $\mathfrak{M} \models \exists y < t(c)\, \phi(c,y)$ となり，$\mathfrak{M} \models T$ に矛盾．

$\mathfrak{M}' \models \neg\exists y\, \phi(c,y)$ なので，$\mathfrak{M}' \models \neg\forall x\, \exists y\, \phi(x,y)$. $\mathfrak{M}'$ は $\mathrm{I}\Delta_0$ のモデルなので $\mathrm{I}\Delta_0 \nvdash \forall x\, \exists y\, \phi(x,y)$. □

指数関数 $y = 2^x$ のグラフは Δ_0 でも表現でき，$2^{x+y} = 2^x \cdot 2^y$ などの指数関数の基本的な性質が $\mathrm{I}\Delta_0$ 上で証明可能なことが知られている．しかし，$\mathrm{I}\Delta_0$ では $\forall x\, \exists y\, (y = 2^x)$ は証明できない．このことが $\mathrm{I}\Delta_0$ 上で初等的な自然数の命題の証明可能性などを考えるときの難しさの原因になっている．たとえば，素数が無限に存在することのユークリッドによる有名な証明はそのままでは $\mathrm{I}\Delta_0$ 上での証明に書き直せない．この，$\mathrm{I}\Delta_0$ 上で素数が無限に存在することを証明できるかどう

かは $I\Delta_0$ に関する重要な未解決問題の一つである (**ウィルキーの問題**). この問題の解決は数学基礎論の枠組みを越え，伝統的な数論での立場とは異なる，自然数上の素数の分布についての新しい視点を与える可能性を持つ．

なお，ここでは簡単のため ϕ が二つの自由変数 x, y を持つ場合についてパリクの定理を証明したが，x, y がそれぞれ変数の列 $\overrightarrow{x}$, $\overrightarrow{y}$ からなる場合もパリクの定理は同様に証明できる．

17.2 P, NP, co-NP

紙テープと，その紙テープ上の文字を読んだり書いたりするヘッド，そして紙テープ上の文字に応じてヘッドの動作を定める単純な制御部からなる計算機を**決定性チューリング機械** (deterministic Turing machine) という．この決定性チューリング機械というのは，いわば理想化された，素朴で古風な架空の計算機であるが，すべての再帰的関数を計算する能力を持つ．この決定性チューリング機械を用いて何ステップで計算できるかによって，関数の計算に必要な時間を測ることを考える．

自然数 x に対して x を二進数表現したときの桁数を $|x|$ と書く．X を自然数の集合とする．うまく決定性チューリング機械を作ると，自然数 x が与えられたとき $|x|$ の多項式時間で x が X に入るかどうかを判定できるときに，X は決定性チューリング機械で多項式時間で計算可能な集合，もしくは **P 集合**という．P 集合であることを現実に計算可能とする立場をとる．

さて，答えを見つけるのは難しくても，答えの候補が与えられたときに，それが正解かどうかの判定することはそれ程難しくない問題がある．たとえば素数の集合 PRIME が P 集合かどうかは今のところ知られていないので，その補集合，つまり合成数の集合 COMPOSITE も P 集合かどうかは分からない．しかし，自然数とその素因数分解の候補が与えられたとき，それが素因数分解になっているかどうかを判断するためにはその候補を掛け合わせてみればいいので，それ程時間はかからない．こうした問題は，複数ある計算の選択肢を同時に確認していけるなら短時間で答を見付けられる．しかし一般には通常の計算機にそうした動作は

許されない．そこで，一つの作業を終えたとき，次の動作の候補が複数個あるような計算機を考える．こうした考え方で決定性チューリング機械を拡張したものが**非決定性チューリング機械 (non-deterministic Turing machine)** である．X を自然数の集合とする．うまく非決定性チューリング機械を造り，入力 x に対して「次に何をすべきか」を「適切に」選びながら計算を進めたときに $|x|$ の多項式時間で x が X に入るかどうか判定できるときに，X は非決定性チューリング機械で計算可能な集合，もしくは **NP 集合**であるといい，補集合が NP 集合となる集合を **co-NP 集合**という．たとえば COMPOSITE は NP 集合であり，PRIME は co-NP 集合である．P 集合全体，NP 集合全体，co-NP 集合全体からなる集合をそれぞれ P, NP, co-NP と書く．

明らかに P 集合は NP 集合である．そして，たとえば PRIME のように P 集合かどうかわからなくても NP 集合であることを示すことは難しくないことも多い．しかし，NP 集合であるが P 集合でないような集合はまだ見つかっていない．そこで次の問題が生じる．

P = NP 問題：P = NP か？

P 集合でない NP 集合の存在が予想されているが，現在のところ未解決である．この P = NP 問題の周辺には重要な未解決問題が数多くあり，その中の一つに NP = co-NP か，という問題がある．P 集合の補集合もまた P 集合なので，P = NP であれば NP = co-NP となる．

NP 集合のなかには特に **NP 完全 (NP-complete)** と呼ばれている集合がある．NP 完全な集合とは，もしもその集合が P 集合ならば P = NP がいえる NP 集合である．NP 完全な集合はクックによって最初に発見され，以後，数多くの NP 完全な集合が発見されている．

次節では NP 集合，NP 完全な集合に関する次の定理を用いる．((1), (2) は計算量理論の標準的な教科書には載っている．(3) は [6] を参照のこと．)

定理 17.3 (1) $\theta(\overrightarrow{x}, \overrightarrow{y})$ が開論理式，$p(\overrightarrow{y})$ が多項式のとき，

$$\{\overrightarrow{a} \text{ は自然数} : \mathfrak{N} \models \exists \overrightarrow{y}(|\overrightarrow{y}| < p(|\overrightarrow{a}|))\psi(\overrightarrow{a}, \overrightarrow{y})\}$$

は NP 集合．

(2) NP 完全な co-NP 集合が存在すれば，NP = co-NP.

(3) $\{(a,b,c) \in \mathbf{N}^3 : \mathfrak{N} \models \exists x \, \exists y \, (ax^2 + by = c)\}$ は NP 完全な集合．

17.3 ウィルキーの定理

ϕ を開論理式とするとき，$\exists x_1 \cdots \exists x_n \, \phi$ の形の論理式を **$\exists_1$論理式**という．マティヤチェビッチ (Yu.V. Matijacevič) はデービス (M. Davis), ロビンソン (J. Robinson), パットナム (H. Putnam) の結果をもとにすべての Σ_1論理式は $\mathfrak{N}$ 上で $\exists_1$論理式と同値であることを示した．このことから「整数係数の不定方程式が解を持つかどうか判定するアルゴリズムは存在しない」ということが示され，ヒルベルトの第 10 問題が否定的に解決された．マッキンタイアはマティヤチェビッチの結果の「$\mathfrak{N}$ 上で」という条件を「$\mathrm{I}\Delta_0$ 上で」という条件に弱められるかという問題を提示した．

マッキンタイアの問題：任意の Σ_1論理式 $\phi(\overrightarrow{x})$ に対し $\exists_1$論理式 $\psi(\overrightarrow{x})$ が存在して，$\mathrm{I}\Delta_0 \vdash \forall \overrightarrow{x}(\phi(\overrightarrow{x}) \leftrightarrow \psi(\overrightarrow{x}))$ となるか？

ウィルキーは，この問題を肯定的に解くことができれば，NP = co-NP がいえることを示した．以下で，このウィルキーの定理を証明する．

任意の Σ_1論理式 $\phi(\overrightarrow{x})$ に対し，同じ数の自由変数を持つ $\exists_1$論理式 $\psi(\overrightarrow{x})$ が存在して $\mathrm{I}\Delta_0 \vdash \forall \overrightarrow{x}(\phi(\overrightarrow{x}) \leftrightarrow \psi(\overrightarrow{x}))$ となることを仮定する．

$$A = \{(a,b,c) \in \mathbf{N}^3 : \mathfrak{N} \models \exists x \exists y \, (ax^2 + by = c)\}$$

とおく．定理 17.3 で述べたように A は NP 完全．よって A が co-NP 集合であることがいえればいい．

明らかに任意の自然数 a, b, c について，$(a,b,c) \in A$ と $\mathfrak{N} \models \exists x < c\, \exists y < c(ax^2 + bx = c)$ は同値．よって $\phi(u,v,w)$ を

$$\phi(u,v,w) \;\Leftrightarrow\; \neg(\exists x < w\, \exists y < w(ux^2 + vy = w))$$

と定めると，任意の自然数 a, b, c について $(a,b,c) \notin A$ と $\mathfrak{N} \models \phi(a,b,c)$ は同値．ゆえに ϕ が定める集合が NP 集合となることを示せばよい．

まず，仮定より開論理式 $\psi(u,v,w,\overrightarrow{z})$ が存在して

$$\mathrm{I}\Delta_0 \vdash \forall u\, \forall v\, \forall w\, (\phi(u,v,w) \leftrightarrow \exists \overrightarrow{z}\, \psi(u,v,w,\overrightarrow{z})).$$

このとき

$$\mathrm{I}\Delta_0 \vdash \forall u\, \forall v\, \forall w\, \exists \overrightarrow{z}(\phi(u,v,w) \rightarrow \psi(u,v,w,\overrightarrow{z})).$$

$\phi(u,v,w) \rightarrow \psi(u,v,w,\overrightarrow{z})$ は Δ_0論理式なのでパリクの定理から $\mathcal{L}_A$ の項 $t(u,v,w)$ が存在して，

$$\mathrm{I}\Delta_0 \vdash \forall u\, \forall v\, \forall w\, \exists \overrightarrow{z} < t(u,v,w)\, (\phi(u,v,w) \rightarrow \psi(u,v,w,\overrightarrow{z})).$$

よって

$$\mathrm{I}\Delta_0 \vdash \forall u\, \forall v\, \forall w\, (\phi(u,v,w) \rightarrow \exists \overrightarrow{z} < t\,(u,v,w)\, \psi(u,v,w,\overrightarrow{z})).$$

さて，この $t(u,v,w)$ に対して多項式 $p(u,v,w)$ を適当に選ぶと任意の自然数 n について $n < t(a,b,c)$ ならば $|n| < p(|a|,|b|,|c|)$. このとき任意の自然数 a,b,c について，$\mathfrak{N} \models \phi(a,b,c)$ と $\mathfrak{N} \models \exists \overrightarrow{z}(|\overrightarrow{z}| < p(|a|,|b|,|c|))\psi(a,b,c,\overrightarrow{z})$ は同値．これは ϕ が定める集合が NP 集合であることを示す．よって A は co-NP 集合．以上でウィルキーの定理が証明された．

このウィルキーの定理は $\mathrm{I}\Delta_0$ と計算量理論との結び付きの端緒に過ぎない．バス，竹内らの証明論的手法による限定算術の展開などにより，$\mathrm{I}\Delta_0$ 周辺の体系と計算量理論の関係に関する数多くの重要な結果が得られている．([2, 7, 8, 9, 10] を参照のこと．)

パートD参考文献

パートDでは以下の教科書，論文を参照した．

[1] Kaye, R. *Models of Peano Arithmetic* (Oxford Univ. Press, 1991 年).

[2] Hajék and Pudlák, *Metamathematics of First-Order Arithmetic* (Springer-Verlag, 1993 年).

[3] Jech, T. *Set Theory* (Academic Press, 1978 年).

[4] Jech, T., *On Gödel's second incompleteness theorem*, Proceedings of American Mathematical Society (1994) 121, 311–313.

[5] Smoryński, C., *The incompleteness theorems*, Handbook of Mathematical Logic (J. Barwise 編，North-Holland, 1977 年) 821–865.

[6] Manders, K.L., *Computational complexity of decision problems in elementary number theory*, Model Theory of Algebra and Arithmetic, Lecture Notes in Mathematics 834 (L. Pacholski 他編，Springer, 1980 年) 211–227.

[7] 竹内外史 著『証明論と計算量』(裳華房，1995 年).

[8] 竹内外史 著『P と NP』(日本評論社， 1996 年).

[9] Krajíček, J. *Bounded Arithmetic, Propositional Logic, and Complexity Theory* (Cambridge Univ. Press, 1995 年).

[10] Buss, S.R. *Bounded Arithmetic* (Bibliopolis, 1986 年).

[1] は算術の超準モデルに関する標準的な教科書である．最近の話題よりも古典的な話に重点が置かれており，よくまとまっていて読みやすい．[2] はより広く，論理の枠組みの中での算術の話題全般に関する教科書と言えるが，話題が豊富な分だけ読みにくい面もある．第 14 講の内容については [1, 2] に詳しい．第 15 講のテンネンバウムの定理の証明は [1] による．第 16 講で紹介した超準モデルを用いての不完全性定理の証明は最近の，ある意味では特種な話題なのでこうした教科書には載っていないが，算術化された完全性定理については [1] にも解説がある．現在の研究の算術の公理系の話題の中心の一つは，第 17 講でもその一端を紹介した計算量理論との関係であろう．この話題についての教科書，参考書に [2, 7, 8,

9, 10] がある．[10] は証明論の手法による限定算術の古典であり，[2] には [10] の結果のモデル論的な証明なども載っている．[10] や [2] に対して [9] にはごく最近の研究課題に密接した話題が数多く紹介されているが，多くの予備知識が仮定されている．限定算術の日本語の教科書に [7] と [8] がある．[7] は [10] にある限定算術の基本的な結果の紹介と，限定算術と命題論理の関係についてのいくつかの話題からなる．[8] には計算量理論についての比較的最近の結果や，著者自身による限定算術の最先端の研究の紹介がある．第 17 講のパリクの定理の証明やウィルキーの定理の証明は [2] による．

補講　不完全性定理を超えて

ヒルベルトのプログラム

まず,「ヒルベルトの還元主義プログラム」について簡単に説明しておこう．ヒルベルトの思想は，1910 年代から 20 年代に勢力を増大させていた直観主義との論争において気迫のこもった鋭い言葉で表現されている．当時，数学界のリーダーであったヒルベルトは，これまで人類が何千年もかけて築き上げてきた数学の世界が，ブラウワーらの主張の如く単なる虚構であるとは考えられなかった．ブラウワーら直観主義者が数学における非構成的な手法を攻撃してきたのに対し，彼は猛然と反撥し，非構成的な証明法を養護する数学の哲学を打ち立てた．彼の主張は，数学はその内容がいかに非構成的でも，きちんとした証明を与えれば証明自体は有限の文字列に過ぎないから，いわゆる「有限の立場」でその正当性が確かめられるというものである．

数学全体が議論できるような大きな体系 T (例:集合論 ZFC) についても，その証明可能性はある文字列 (公理) が別の文字列 (定理) に有限的に変換できるかどうかの問題である．だから，たとえばフェルマーの定理 ($\forall n > 2\, \forall x, y, z(x^2 + y^2 \neq z^2)$) のように集合の存在を何も主張しない命題 ($\Pi^0_1$命題) に対しては，もし T で証明があるなら，その証明の構造をじっと眺めれることで,「有限の立場」での証明も抽出できるはずだと彼は考えた．

大きな体系 T に対し，その体系の記号操作ができる程度の小さな体系 (例:PRA) を t として，われわれは次の図式 (を証明すること) をヒルベルトの計画 HP と呼ぶことにする：

任意の Π^0_1命題 φ に対し，$T \vdash \varphi$ ならば $t \vdash \varphi$.

以下，T も t も少なくとも原始再帰的算術 PRA または $\mathrm{I}\Sigma_1$ を含むとしておく．

補題．任意の Π^0_1命題 φ に対し，$T \vdash \varphi$ ならば $t + \mathrm{Con}(T) \vdash \varphi$.

[証明] φ を Π^0_1命題とし，$T \vdash \varphi$ を仮定する．すると，$t \vdash \mathrm{Pr}_T(\overline{\ulcorner\varphi\urcorner})$ は容易にい

える (定理 6.1)．他方，$\neg\varphi$ は Σ^0_1命題だから，$t \vdash (\neg\varphi \to \mathrm{Pr}_T(\ulcorner\neg\varphi\urcorner))$ (定理 9.4 を参照)．よって，$t \vdash (\neg\varphi \to \neg\mathrm{Con}(T))$ となるから，$t + \mathrm{Con}(T) \vdash \varphi$ である．□

この定理により，$t \vdash \mathrm{Con}(T)$ ならば，HP がいえることがわかる．そこで，Con(T) を有限の立場で証明することが具体的な目標になるが，これはヒルベルトが直観主義との論争以前からその重要性を強調していた数学の無矛盾性の問題に他ならない．しかし，ゲーデルの不完全性定理によって，Tにおいて (したがって t においても) Con(T) は証明できないことがわかり，この方法で HP を導くことはできない．

いま，T を Con(t) が証明できるほど大きくとると，HP の仮定のもとでは $t \vdash \mathrm{Con}(t)$ となり，これもゲーデルの結果に反する．しかし，T を それ程大きくせず，$t = \mathrm{PRA}$ に対して HP が成立するような理論 $T = \mathrm{WKL}_0$ でもかなりの数学が展開できることが，最近の「逆数学プログラム」でわかってきた．このような事実により,「逆数学」は「ヒルベルトのプログラム」の現代版とか部分的実現とかいわれることがある．

逆数学プログラム

「逆数学」という名の研究プログラムでは，2 階算術という枠組みにおいて，ある定理を証明するのにどの程度の集合存在公理が必要かを調べている．まず，2 階算術について簡単に説明しておこう．自然数を対象とした理論を「1 階算術」といい，自然数と自然数からなる集合の両者を対象とした理論を「2 階算術」という．2 階算術の公理系 Z_2 は，自然数の順序や和積演算に関する 1 階算術の諸公理と，定義し得るどんな自然数の集まりも “集合” として扱えることを保証する集合存在公理 (内包公理) から成り立っている．体系 Z_2 は「実数論」あるいは「解析」とも呼ばれ，一般の数学のかなりの部分がそこで展開できることはヒルベルトとベルナイスの研究以来よく知られている．もちろん，集合論を使えばもっと楽に現代数学のほとんどをカバーできるが，それでは逆に器が大きすぎて本当に必要な公理を特定しにくいのである．

体系 Z_2 の集合存在公理に種々の制限を付けることによりいろいろな部分体系が得られている.「逆数学」において特に重要な体系は (証明能力の) 弱い方から順に, RCA_0, WKL_0, ACA_0, ATR_0, Π^1_1-CA_0 の5つである. これら5つの体系の無矛盾性は証明論においてすでに確立したものと考えられているが, それより本質的に強い集合存在公理を持つ体系の無矛盾性については未だ研究が進行中である.

1974年頃, H. フリードマンは Z_2 の各部分体系でどれだけの数学が展開できるかを調べ, 次のような現象に気付いた:

> 数学の定理の多くは RCA_0 で証明できるか, そうでなければ上にあげた他の4つの体系のどれかと論理的に同値であることが RCA_0において証明できる.

これは「逆数学現象」と呼ばれ, その後もこのパターンに当てはまる数多くの定理が S. シンプソンを中心とする研究グループによって発見されている. しかし, この現象に当てはまらない例も少なからず知られている.

以下, 5つの公理系とそこで証明できる定理の特徴などについて簡単に述べよう.

1. RCA_0. この体系は, 自然数上の基本演算に関する公理と Σ^0_1式に関する帰納法, そして再帰的内包公理と呼ばれる集合存在公理からできている. 荒っぽくいえば, RCA_0で展開される数学は計算機が扱える範囲の数学であり, これは計算可能解析学 (computable analysis) とか再帰的代数学 (recursive algebra) などの形式化にあたる. たとえば, RCA_0 では, 中間値の定理が証明できる. 理由は, 中間値の定理には2分法と呼ばれるアルゴリズムがあって, 任意の $n > 0$ に対し, 誤差 $\pm\frac{1}{n}$ 以内の近似有理解を有限ステップで求めることができるからである.
2. WKL_0. この体系は, RCA_0 に "無限個の頂点を持つ2分木は無限長の道 (path) をもつ" という弱い形のケーニヒの補題 (Weak König's Lemma) を公理として加えたものである. 2分木を有限分岐木に置き換えた命題が一般のケーニヒの補題で, これは次に述べる ACA_0と同値になる. WKL_0 では, カントル空間 $\{0,1\}^{\mathbf{N}}$ のコンパクト性や実閉区間 [0, 1] のコンパクト性 (ハイネ-ボレルの定理) が導け, さらにそれらと WKL_0 との同値性も RCA_0

で証明できる．コンパクト性の助けによって，WKL_0 で展開される数学は RCA_0 上の数学よりずっと豊かで，かつ数学的に自然なものになる．しかし，証明論的には，つまり無矛盾性に関しては2つの体系は同等であり，上でも述べたように WKL_0 (および RCA_0) と PRA の間には HP の図式が成立している．

3. ACA_0. 集合に関する量化記号 ($\forall X$, $\exists X$) を含まない論理式を算術的という．算術的内包公理 (Arithmetical Comprehension Axiom) は，算術的論理によって定義される集合の存在を主張するもので，この公理を RCA_0 加えてできる体系が ACA_0 である．算術的内包公理と同値になる定理には，ボルツァーノ・ワイエルシュトラスの定理，可算ベクトル空間の基底の存在などがある．また，ACA_0はペアノの1階算術 PA の保存的拡大 (conservative extension) になっている．つまり，PA の定理は ACA_0 で証明でき，ACA_0 で証明できる1階算術の命題は PA の定理になる．
4. ATR_0. 算術的内包公理を超限回繰り返して得られる集合の存在を主張するのが算術的超限再帰 (Arithmetical Transfinite Recursion) の公理であり，これを RCA_0 に加えたものが ATR_0 である．この超限操作は，開集合のクラス $\mathbf{G}$ から始めて，可算集合演算によって $\mathbf{G}_\delta, \mathbf{G}_{\delta\sigma}, \cdots$ のようにボレル集合を構成してゆく手続きに相応するもので，スースリンの分離定理など記述集合論のいろいろな定理がこの体系と同値なる．
5. Π^1_1-CA_0. ϕ を算術的論理式としたとき，$\forall X\ \phi$ を Π^1_1論理式と呼び，この形の式で定義される集合の存在を要請する公理を RCA_0 に加えたものが，Π^1_1-CA_0 である．この体系と同値になる定理には，任意の可算アーベル群が最大加除部分群を直積因子にもつというウルムの定理などがあるが，ここまで強い公理を必要とする普通の数学の定理はむしろ少ない．

おわりに

不完全性定理はオール・マイティーではない．最後に，2つばかり注意を述べてこの本の締めくくりとしよう．本書でほとんど扱えなかった大切な話題に限定算術

(bounded arithmetic) がある．体系 $I\Delta_0$ に指数関数を加えた体系を $I\Delta_0+\exp$ と書くが，限定算術の話では普通これが最強の体系である．にもかかわらず，$I\Delta_0+\exp$ で $Con(Q)$ が証明できないことが知られている．$I\Delta_0+\exp$ と Q の間にはさまざまな体系があり，それらの体系の強弱を知ることが限定算術の主要な関心事なのだが，このときお互いどうしの無矛盾性はまったく証明できないことになるから，第 2 不完全性定理は，それが成り立つにせよ，そのままでは体系の強弱を決定するのにまったく無力である．蛇足かもしれないが，$I\Delta_0+\exp$ と Q の間に HP が成り立っていないことは容易にわかる．

もう一つ，数学の世界には完全な公理系も不完全な公理系もたくさんあることを忘れてはいけない．実数，複素数には完全な公理系があり，自然数，整数や有理数にはそれがない．本文でも述べたように，自然数の体系も掛け算をとって，足し算と不等号だけにすれば再帰的に公理化可能である．逆に，実数体に指数関数を入れた場合に完全な公理系があるかどうかはまだわかっておらず，この辺は数学基礎論の研究最前線の話題の一つである．

索 引

田中一之 (たなか・かずゆき)

Ph.D.(カリフォルニア大学バークレイ校，1986)

東京工業大学理学部助手を経て，

現在，東北大学大学院理学研究科助教授.

著書：『計算理論と論理プログラミング』(共訳) 丸善.

鹿島 亮 (かしま・りょう)

博士 (理学)(東京工業大学，1995)

東京工業大学大学院情報理工学研究科助手を経て，

現在，北陸先端科学技術大学院大学情報科学研究科助手.

角田法也 (かどた・のりや)

博士 (学術)(広島大学，1992)

広島大学工学部助手を経て，

現在，熊本大学工学部講師.

菊池 誠 (きくち・まこと)

博士 (理学)(東北大学，1996)

現在，神戸大学大学院自然科学研究科助手.

数学基礎論講義 — 不完全性定理とその発展

1997 年 3 月 10 日　第 1 版第 1 刷発行

著　者：田中一之 (編・著) /鹿島 亮/角田法也/菊池 誠

発行者：大石 進

発行所：株式会社 日本評論社

：〒170 東京都豊島区南大塚 3-12-4

：電話 03-3987-8621 (販売) -8599 (編集)

制　作：株式会社 プレイン

印　刷：壮光舎印刷株式会社

製　本：誠製本株式会社

装　丁：杉田ゆみ /イラスト：清水幸枝

ISBN 4-535-78241-5